MICE Management Manual

INDUSTRIAL ETHERNET

Modular Industrial Communication Equipment

MICE Management Manual

INDUSTRIAL ETHERNET

Modular Industrial Communication Equipment

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and trade name protection law and hence that they may be freely used by anyone.

© 2002 Hirschmann Electronics GmbH & Co. KG

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is formed by the preparation of a backup copy of the software for your own use.

This manual has been created by Hirschmann Electronics GmbH & Co. KG according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this manual.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. For the rest, we refer to the conditions of use specified in the license contract.

Printed in Germany

Hirschmann Electronics GmbH & Co. KG
Automation and Network Solutions
Stuttgarter Straße 45-51
D-72654 Neckartenzlingen
Tel.: ++49-7127-14-1538

039 650-002-01-0502

Hirschmann worldwide:

Germany

Hirschmann Electronics GmbH & Co. KG
Automation and Network Solutions
Stuttgarter Straße 45-51
D-72654 Neckartenzlingen
Tel. ++49-7127-14-1527
Fax ++49-7127-14-1542
e-mail: ans-hi-line@nt.hirschmann.de
Internet: www.hirschmann.de

Austria

Hirschmann Austria GmbH
Oberer Paspelweg 6-8
A-6830 Rankweil-Brederis
Tel. ++43-5522-3070
Fax ++43-5522-307555
email: info@rw.hirschmann.at

Switzerland

Hirschmann Electronics GmbH & Co. KG, Neckartenzlingen
Zweigniederlassung Uster
Seestr. 16
CH-8610 Uster
Tel. ++41-1905-8282
Fax ++41-1905-8289
mail: ans_ch@hirschmann.ch

France

Hirschmann Electronics S.A.
24, rue du Fer à Cheval, Z.I.
F-95200 Sarcelles
Tel. ++33-1-39330280
Fax ++33-1-39905968
e-mail: ans@hirschmann.fr

Great Britain

Hirschmann Electronics Ltd.
St. Martins Way
St. Martins Business Centre
GB-Bedford MK42 OLF
Tel. ++44-1234-345999
Fax ++44-1234-352222
e-mail: enquiry@hirschmann.co.uk

Netherlands

Hirschmann Electronics B.V.
Pampuslaan 170
NL-1382 JS Weesp
Tel. ++31-294-462591
Fax ++31-294-462554
e-mail: ans@hirschmann.nl

Spain

Hirschmann Electronics S.A.
Calle Traspaderne, 29
Barrio del Aeropuerto
Edificio Barajas 1,2 Planta
E-28042 Madrid
Tel. ++34-1-7461730
Fax ++34-1-7461735
e-mail: hes@hirschmann.es

Hungary

Hirschmann Electronics Kft.
Rokolya u. 1-13
H-1131 Budapest
Tel. ++36-1-3494199
Fax. ++36-1-3298453
e-mail: hirschmann.budapest@axelero.hu

USA

Hirschmann Electronics Inc.
30 Hook Mountain Road _ Unit 201
USA-Pine Brook, N. J. 07058
Tel. ++1-973-8301470
Fax ++1-973-8302000
e-mail: ans@hirschmann-usa.com

Singapore

Hirschmann Electronics Pte. Ltd.
3 Toh Tuck Link
04-01 German Districentre
Singapore 596228
Tel: +65-6463 5855
Fax:+65-6463 5755
e-mail: hirschmann.svi@pacific.net.sg

Contents

1 Introduction 17

1.1 Designed for industrial use, flexible, efficient and equipped for the future 19

1.1.1 Networks for the Future 19
1.1.2 Intelligent networking 20
1.1.3 Reliability is the bottom line 21
1.1.4 The highest degree of flexibility 22
1.1.5 User-friendly startup and user-friendliness 23

1.2 Easy-to-operate management system 25

2 Hardware 27

2.1 MICE 2000 MS2108 - 2 switch 29

2.1.1 MICE 2000 MS2108 - 2 switch 30
2.1.2 MICE 3000 MS3124 - 4 switch 31

2.2 MICE 2000 media modules 33

2.2.1 MM2 - 2FLM4 33
2.2.2 MM2 - 4TX1 34
2.2.3 MM2 - 4FXM3 35
2.2.4 MM2 - 2FXM3 / 2TX1 36
2.2.5 MM2 - 2FXM2 37
2.2.6 MM2 - 2FXS2 38

2.3 MICE 3000 media modules 39

2.3.1 MM3 - 4FLM4 39
2.3.2 MM3 - 2FXM2/2TX1 40
2.3.3 MM3 - 2FXS2/2TX1 41
2.3.4 MM3 - 1FXL2 / 3TX1 42
2.3.5 MM3 - 4FXM2 43

2.4 MB3 - 2T expansion module 45

3 Installation and startup procedure 47

3.1 Security instructions 49

3.2 Device installation 53

3.2.1 Controls 53
3.2.2 6-pin terminal block 54
3.2.3 Assembly 56
3.2.4 Interfaces 58
3.2.5 Disassembly 60

3.3 Startup operation 61

3.4 Basic settings 63

3.4.1 System configuration 71
3.4.2 IP Address 72

3.5 tftp server for software updates 77

3.5.1 Setting up the tftp process 78
3.5.2 Software access rights 81

3.6 System monitors 83

3.6.1 Update of the operating system (System monitor 1) 83
3.6.2 Software update (System monitor 2) 90

4 Functions 95

4.1 Hardware functions 97

4.1.1 Diagnostics 97
4.1.2 Autonegotiation 97
4.1.3 Autopolarity Exchange 98
4.1.4 Autocrossing 98
4.1.5 Line monitoring 98
4.1.6 Reset 99

4.2 Display indicators 101

4.2.1 Device status 101
4.2.2 Display status 102
4.2.3 Port status 104

4.3 Frame switching 107

4.3.1 Store and Forward 107
4.3.2 Multi-address capability 107
4.3.3 Learning addresses 108
4.3.4 Prioritization 108
4.3.5 Tagging 109

4.4 Redundancy 111

4.4.1 Line configuration 111
4.4.2 Redundant ring structure – HIPER-Ring 112

4.5 GMRP 113

4.6 Security 115

4.6.1 Port security 115
4.6.2 SNMP 116
4.6.3 SNMP Traps 117
4.6.4 SNMP traps when booting 118

5 Web-based management 119

5.1 Opening the Web-based interface 121

5.2 Menu tree 125

5.3 System 127

5.3.1 Updating the software 132
5.3.2 Defining the start configuration 135
5.3.3 Configure the network 138
5.3.4 Password 139
5.3.5 Security 141
5.3.6 Access for IP addresses 142
5.3.7 Configuring traps 144
5.3.8 Restarting the switch 145

5.4 Port 147

5.4.1 Port Configuration Table 147
5.4.2 Port Statistic Table 149

5.5 Switching 151

5.5.1 Filtering Database 151
5.5.2 GMRP 152

5.6 Extras 155

5.6.1 Configuring the HIPER-RING function 156
5.6.2 Setting port mirroring 157
5.6.3 Switching the learning function on and off 158
5.6.4 Setting port security 159

6 Management Information Base MIB 161

6.1 MIB II 165

6.1.1 System Group (1.3.6.1.2.1.1) 165
6.1.2 Interface Group (1.3.6.1.2.1.2) 168
6.1.3 Address Translation Group (1.3.6.1.2.1.3) 169
6.1.4 Internet Protocol Group (1.3.6.1.2.1.4) 169
6.1.5 ICMP Group (1.3.6.1.2.1.5) 171
6.1.6 Transfer Control Protocol Group (1.3.6.1.2.1.6) 172
6.1.7 User Datagram Protocol Group (1.3.6.1.2.1.7) 173
6.1.8 Simple Network Management Protocol Group (1.3.6.1.2.1.11) 173
6.1.9 RMON Gruppe (1.3.6.1.2.1.16) 174
6.1.10 dot1dBridge (1.3.6.1.2.1.17) 177
6.1.11 MAU Management Group (1.3.6.1.2.1.26) 179

6.2 Private MIB 181

6.2.1 Device group 181
6.2.2 Management group 184
6.2.3 User groups group 186
6.2.4 HIPER-Ring redundancy group 186

7 User Interface 187

7.1 Starting the User Interface 189

7.2 Working with the User Interface 191

7.2.1 System parameters 191
7.2.2 Switch Security 194
7.2.3 Port Configuration / Statistics 195
7.2.4 Port Mirroring / Disable Learning 196
7.2.5 Configuration 197
7.2.6 Updating 200
7.2.7 Password 201
7.2.8 Ping 202
7.2.9 System Reset 203

A Appendix 205

FAQ 207

Based specifications and standards 209

Certifications 211

Technical Data 213

Literature references 217

Reader's comments 219

Index 221

1 Introduction

In 1984 Hirschmann created the first fiber optic Ethernet network at the University of Stuttgart. In 1990 Hirschmann also invented the "Redundant Ethernet Ring".

These innovations were followed by the first media converter for fieldbuses in 1993 and a HIPER-Ring for shared Ethernet networks in 1998.

Today this global specialist for company-wide networks offers Ethernet/Fast-Ethernet transceivers, hubs, switches, routers as well as Gigabit Ethernet switches and a standard management software package for all network components.

1.1 Designed for industrial use, flexible, efficient and equipped for the future

1.1.1 Networks for the Future

Communications in the field of automation is ever-changing. There used to be a time when networks were implemented according to hierarchical levels and interconnected with gateways.

Today open and transparent system solutions are demanded. The availability and the ability to integrate existing information is playing an increasingly important role.

In the office environment, Ethernet networks have a market share of greater than 80%. Similar developments can now be witnessed in the field of industrial automation.

There too, leading manufacturers are developing components designed to run on Ethernet-based systems.

The Hirschmann INDUSTRIAL products, which include the MICE and the Rail family, were developed specifically for the demanding requirements of industrial automation.

Both product families, complemented by the MACH 3000 and the HiWay products, ensure integrated communication over all levels of the enterprise.

1.1.2 Intelligent networking

Hirschmann Electronics' MICE sets new standards in industrial Ethernet networking.

Whether it is used in a control cabinet or decentral in a distribution box, the MICE family allows you to combine functions meet your specific needs.

Currently available are switches and media modules supporting the standards:

- 10BASE-T
- 10BASE-FL
- 100BASE-TX
- 100BASE-FX.

All terminal devices and other infrastructure components can be connected via:

- Twisted-pair cables,
- Multimode F/O cables,
- Singlemode F/O cables

The modular switches are easy to install – simply snap them onto a DIN-rail (this also provides the functional grounding) and plug the media modules onto the switch.

1.1.3 Reliability is the bottom line

To guarantee the highest degree of operating reliability, our products fulfill all relevant industrial standards regarding EMI emission, EMI immunity, vibration, shock, operating temperatures, etc. In addition, our switches are fan-less, can be powered redundantly, and support the HIPER-Ring. All of these features contribute to a high level of reliability.

The network can be compared to an Achilles heel. If it is interrupted, certain functions are no longer possible. As a consequence, an interruption in the communication network of a plant inevitably leads to productions losses. For this reason, network availability has become a very important factor.

With the HIPER-Ring, Hirschmann Electronics has developed a redundancy concept that is characterized by

- very fast network reconfiguration
- greatly simplified network planning
- the need for only one additional link (to close the ring)

The HIPER-Ring is supported by the MACH, Rail and MICE product families. This ensures a very high degree of availability in every area of a network. The individual areas can also be reliably interconnected using redundancy procedures such as dual homing and redundant networking coupling.

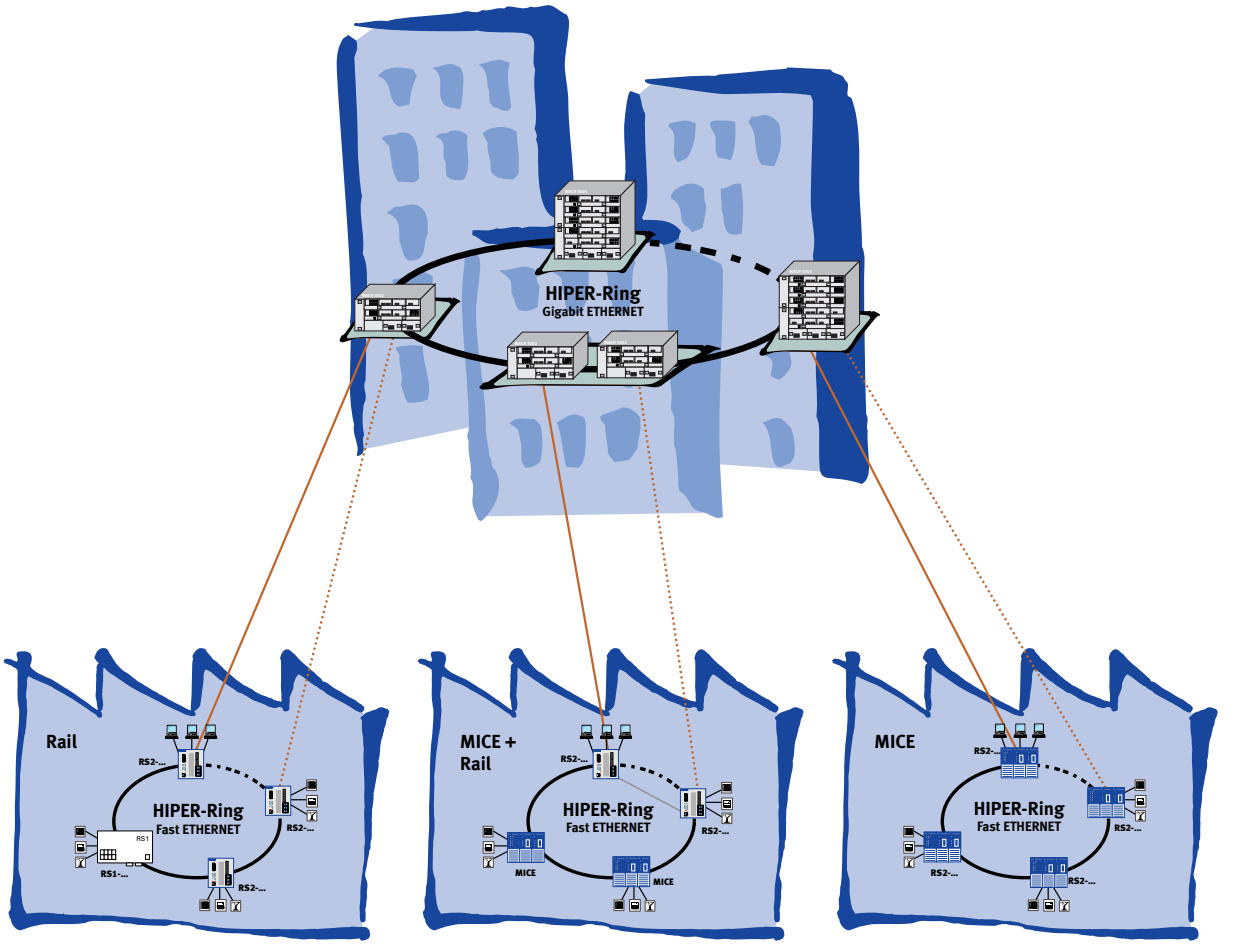


Fig. 1: High reliable

1.1.4 The highest degree of flexibility

The modular architecture is just one of the many outstanding features of MICE. It allows you to individually combine functions and Ethernet connections according to your needs.
The modular architecture also safe-guard your investment. Because the MICE concept guarantees availability for many years and the maximum of flexibility - not only for today's needs, but also for those of tomorrow.

1.1.5 User-friendly startup and user-friendliness

With the large labels you can clearly identify the modules which in turn lets you make the proper connections quickly and correctly. The labels may be printed or written by hand and may be easily replaced at any time.
This facilitates a simplified startup and commissioning, effectively saving you time and money.

The diagnostic LEDs and the connectors are separated which provide an unobstructed view of the indicators – even when all of the ports are connected.

Another feature is the selectable operating parameter. This supports user-friendly startup and helps pinpoint any problems quickly and easily.

You decide which parameter is displayed by simply pushing a button.

1.2 Easy-to-operate management system

The MICE switches offer manage your system:

- Locally on the switch (via V.24 interface)
- From any point in the network (via a web browser)
- Centrally, via SNMP management software, e.g. HiVision.

The integrated signal contact offers universal remote diagnostics. The operating state can be monitored by a digital input signal.

2 Hardware

The INDUSTRIAL ETHERNET MICE (Modular Industrial Communication Equipment) family consists of a switch basic module and the media modules. These devices are user-manageable. A switch basic module contains all functions of this industrial switch with the exception of the interfaces for connecting a LAN. Pluggable media modules provide these interfaces. They differ in their number of interfaces and the media type for connecting segments. The various switch basic modules differ in their number of pluggable media modules. An expansion module allows you to add 2 slots to the switch basic modules for installing media modules.

For the sake of simplicity, the switch basic module with the pluggable media modules are referred to as MICE in this manual.

The MICE operates in store-and-forward mode. When a data packet is being received, the MICE analyzes the source and destination addresses. It can store up to 4000 addresses with port allocations in its address table.

The MICE conforms to the specifications of the standards
ISO/IEC 8802-3 10BASE-FL,
ISO/IEC 8802-3u 10BASE-T/-100BASE-TX and
ISO/IEC 8802-3 100BASE-FX

The LEDs indicate data reception, connection status and processor status.

The Hirschmann "Basics INDUSTRIAL ETHERNET and TCP/IP" (order no. 280 720-834) describes in detail
– how to set up a local network in compliance with ISO/IEC 8802-3 and
– provides instructions on network planning as well as on the installation of Ethernet networks.

2.1 MICE 2000 MS2108 - 2 switch

The MICE 2000 MS2108-2 switch and the MICE 3000 MS3124-4 switch are the switch basic modules of the Modular Industrial Communication Equipment. It contains all function elements such as the:

- Switch function,
- Management function,
- Redundancy function,
- Display control,
- Voltage connection,
- Management connection,
- Adjustment elements,
- Slots for media modules.

The MICE 2000 family is designed for use in flat distribution boxes.
The MICE 3000 family is designed for use in distribution boxes and switch cabinets with higher port numbers.
The MICE 2000 and MICE 3000 media modules can be used in both the MICE 2000 MS2108-2 switch and MICE 3000 MS3124-4 switch.

2.1.1 MICE 2000 MS2108 - 2 switch

The MICE 2000 MS2108 - 2 switch features two slots for media modules. Equipped with 4-port media modules, the MICE 2000 MS2108 switch allows you to connect up to

- 8 network segments.

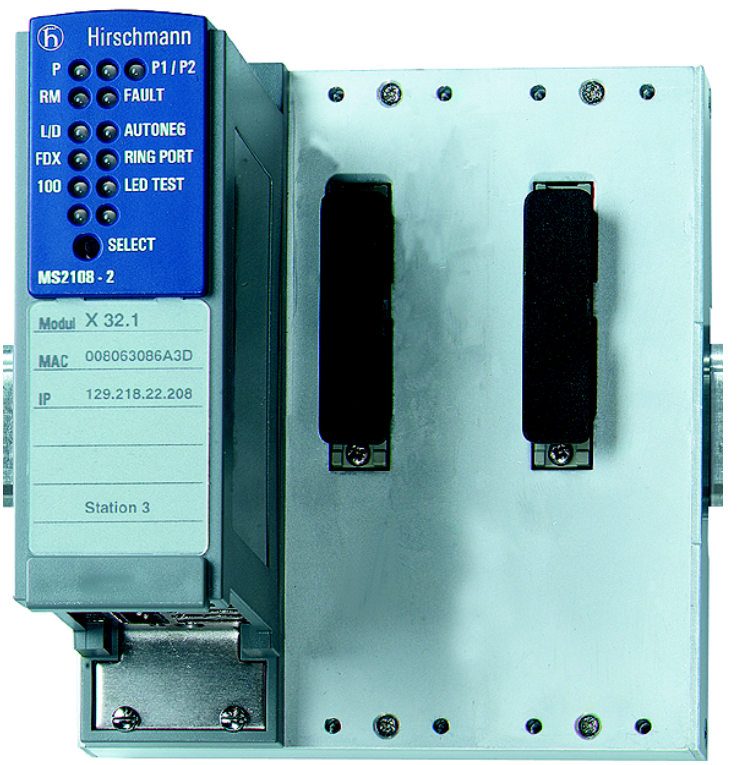


Fig. 2: Front view of the MS2108-2

2.1.2 MICE 3000 MS3124 - 4 switch

Das MICE 3000 MS3124 - 4 switch in the basic version offers four slots for media modules. With the expansion module, you can increase the number of slots by 2.
Equipped with 4-port media modules, the MICE 3000 MS3124 - 4 switch allows you to connect up to

- 16 network segments or
- 24 network segments when using an expansion module.

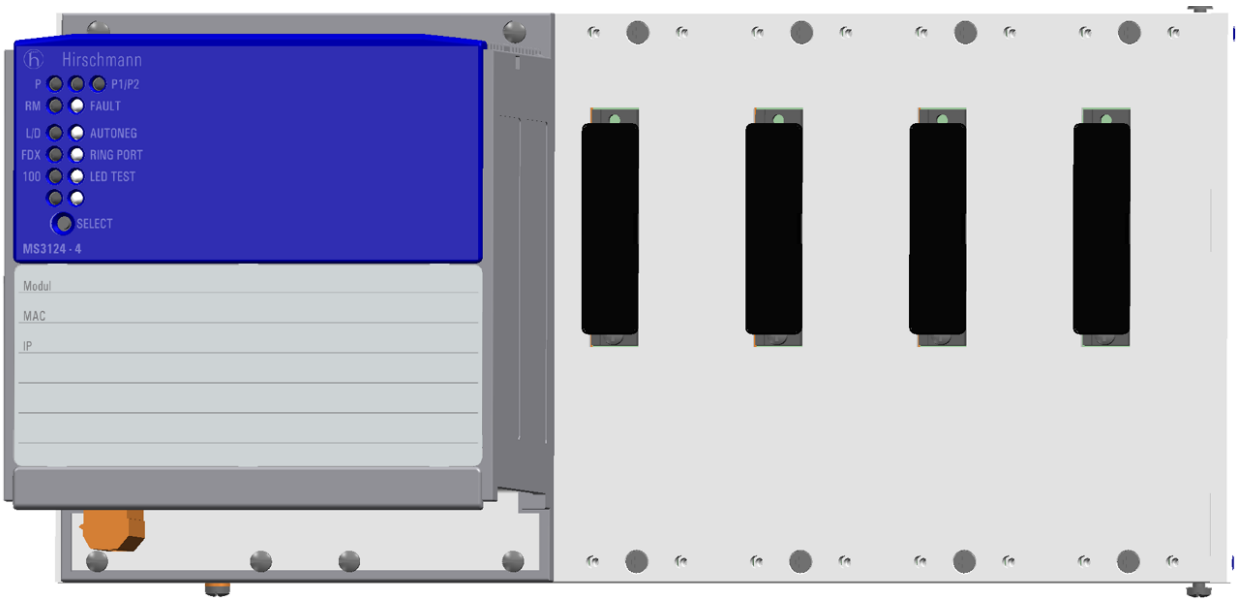


Fig. 3: Frontansicht des MS3124 - 4

2.2 MICE 2000 media modules

2.2.1 MM2 - 2FLM4

The MICE 2000 media modules form the MICE interface to the LAN. The MM2 - 2FLM4 has 2 F/O interfaces.

It allows you to connect up to

- 2 independent multimode F/O segments compliant with 10BASE-FL with an ST connection.

Fig. 4: Front view of the MM2 - 2FLM4

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.2.2 MM2 - 4TX1

The MICE 2000 media module forms the MICE interface to the LAN. The MM2 - 4TX1 has 4 twisted-pair interfaces.

It allows you to connect up to

- 4 independent **T**wisted-**P**air (TP) segments (10BASE-T/100BASE-TX) with an RJ45 connection.

Fig. 5: Front view of the MM2 - 4TX1

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.2.3 MM2 - 4FXM3

The MICE 2000 media module forms the MICE interface to the LAN. The MM2 - 4FXM3 has 4 F/O interfaces.

It allows you to connect up to

- 4 independent multimode F/O segments compliant with 100BASE-FX with an MTRJ-connection.

Fig. 6: Front view of the MM2 - 4FXM3

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.2.4 MM2 - 2FXM3 / 2TX1

The MICE 2000 media module forms the MICE interface to the LAN. The MM2 - 2FXM3 / 2TX1 has 2 F/O interfaces and 2 twisted-pair interfaces.

It allows you to connect up to

- 2 independent multimode F/O segments compliant with 100BASE-FX with a MTRJ connection and
- 2 independent twisted-pair (TP) segments (10BASE-T/100BASE-TX) with an RJ45 connection.

Fig. 7: Front view of the MM2 - 2FXM3 / 2TX1

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.2.5 MM2 - 2FXM2

The MICE 2000 media module forms the MICE interface to the LAN. The MM2 - 2FXM2 has 2 F/O interfaces.

It allows you to connect up to

- 2 independent multimode F/O segments compliant with 100BASE-FX with an DSC connection.

Fig. 8: Front view of the MM2 - 2FXM2

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.2.6 MM2 - 2FXS2

The MICE 2000 media module forms the MICE interface to the LAN. The MM2 - 2FXS2 has 2 F/O interfaces.

It allows you to connect up to

- 2 independent singlemode F/O segments compliant with 100BASE-FX with an DSC connection.

Fig. 9: Front view of the MM2 - 2FXS2

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.3 MICE 3000 media modules

2.3.1 MM3 - 4FLM4

The MICE 3000 media module forms the MICE interface to the LAN. The MM3 - 4FLM4 has 4 F/O interfaces.

It allows you to connect up to

- 4 independent multimode F/O segments compliant with 10BASE-FL with an ST connection.

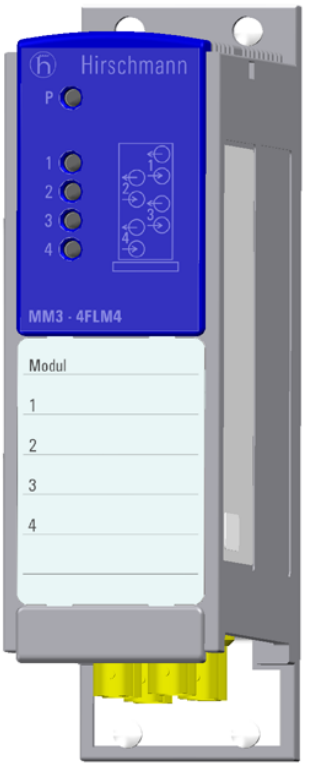


Fig. 10: Front view of the MM3 - 4FLM4

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.3.2 MM3 - 2FXM2/2TX1

The MICE 3000 media module forms the MICE interface to the LAN. The MM3 - 2FXM2/2TX1 has 2 F/O interfaces and 2 twisted-pair interfaces.

It allows you to connect up to

- 2 independent multimode F/O segments compliant with 100BASE-FX with a DSC-connection and
- 2 independent **T**wisted-**P**air (TP) segments (10BASE-T/100BASE-TX) with an RJ45 connection.

Fig. 11: Front view of the MM3 - 2FXM2/2TX1

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.3.3 MM3 - 2FXS2/2TX1

The MICE 3000 media module forms the MICE interface to the LAN. The MM3 - 2FXS2/2TX1 has 2 F/O interfaces and 2 twisted-pair interfaces.

It allows you to connect up to

- 2 independent singlemode F/O segments compliant with 100BASE-FX with a DSC-connection and
- 2 independent **T**wisted-**P**air (TP) segments (10BASE-T/100BASE-TX) with an RJ45 connection.

Fig. 12: Front view of the MM3 - 2FXS2/2TX1

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.3.4 MM3 - 1FXL2 / 3TX1

The MICE 3000 media module forms the MICE interface to the LAN. The MM3 - 1FXL2 / 3TX1 has 1 F/O interface and 3 twisted-pair interfaces.

It allows you to connect up to

- 1 independent singlemode Longhoul F/O segments compliant with 100BASE-FX with a DSC-connection and
- 3 independent **T**wisted-**P**air (TP) segments (10BASE-T/100BASE-TX) with an RJ45 connection.

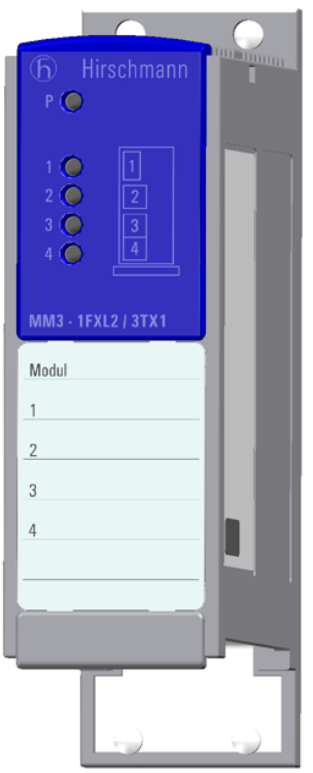


Fig. 13: Front view of the MM3 - 1FXL2 / 3TX1

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.3.5 MM3 - 4FXM2

The MICE 3000 media module forms the MICE interface to the LAN. The MM3 - 4FXM2 has 4 F/O interfaces.

It allows you to connect up to

- 4 independent multimode F/O segments compliant with 100BASE-FX with a DSC-connection

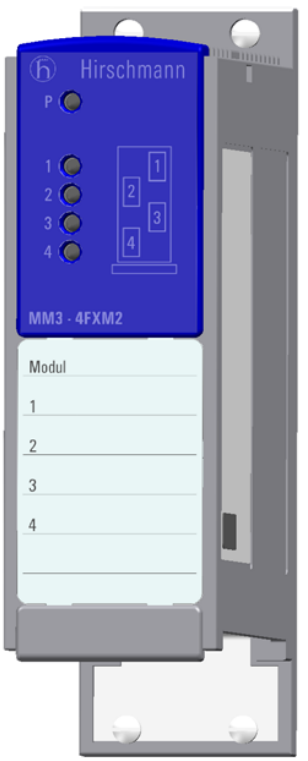


Fig. 14: Front view of the MM3 - 4FXM2

The LEDs also display the data reception and connection status depending on the setting of the switch basic module.

2.4 MB3 - 2T expansion module

The MB3 - 2T expansion module allows you to add 2 slots to the MICE 3000 MS3124 - 4 switch basic module for installing media modules.

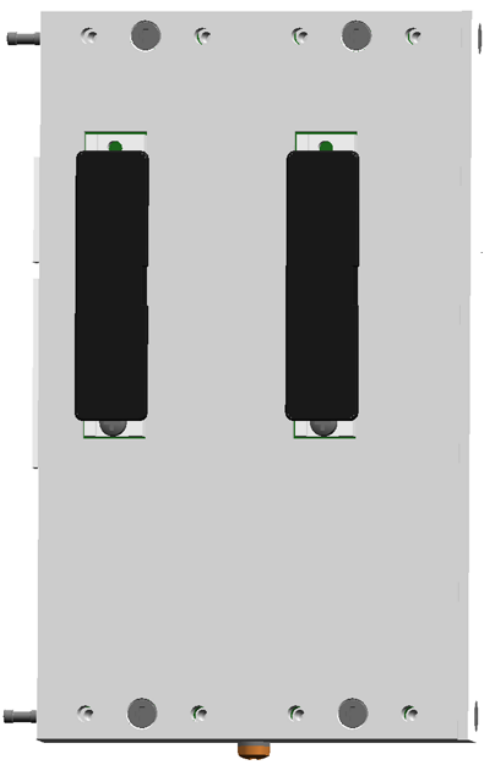


Fig. 15: MB3 - 2T expansion module

3 Installation and startup procedure

The Line INDUSTRIAL ETHERNET Modular Industrial Communication Equipment family has been developed for practical applications in a harsh industrial environment. Accordingly, the installation process has been kept simple.
The few configuration settings required for operation are described in this chapter.

3.1 Security instructions

Supply voltage

The devices are designed for operation with a safety extra-low voltage. They may only be connected to the supply voltage connections and to the signal contact with PELV circuits or alternatively SELV circuits with the voltage restrictions in accordance with IEC/EN 60950.
The supply voltage is electrically isolated from the housing.

- ☐ Never start operation with damaged components!
- ☐ Relevant for North America:
  The subject unit is to be suppplied by a Class 2 power source complying with the requirements of the National Electrical Code, table 11(b).
  If power is redundant supplied (two individual power sources) the power sources together should comply with the requirements of the National Electrical Code, table 11 (b).
- ☐ Relevant for North America:
  Use 60/75°C copper(CU)wire only.

Shielding ground

The shielding ground of the connectable twisted pairs lines is connected to the lower panel as a conductor.

- ☐ Beware of possible short circuits when connecting a cable section with conductive shielding braiding.

Housing

Only technicians authorized by Hirschmann are permitted to open the housing.

The lower covering panel of the housing is grounded by the tophat rail and, as an option, by using the ground screw.

- ☐ The switch basic module forms an inseparable unit. Attempting to remove the display and connection part can damage the switch basic module.
- ☐ Make sure that the electrical installation meets local or nationally applicable safety regulations.
- ☐ The ventilation slits must not be covered to ensure free air circulation.
- ☐ If installed in a living area or office environment, the device must be operated exclusively in switchgear cabinets with fire protection characteristics according to EN 60950.

Ambient conditions

The device may only be operated in an ambient temperature of 0°C to +55°C at a relative air humidity of 10% to 95% (non-condensing).

When an MM2 - 4FXM3 media module is installed, the permitted ambient temperature is 0 °C to +50 °C.

Qualification requirements for the personnel

Qualified personnel as understood in this manual and the warning signs, are persons who are familiar with the setup, assembly, startup, and operation of this product and are appropriately qualified for their job. This includes, for example, those persons who have been:

– trained or directed or authorized to switch on and off, to ground and to label power circuits and devices or systems in accordance with current safety engineering standards;

– trained or directed in the care and use of appropriate safety equipment in accordance with the current standards of safety engineering;

– trained in providing first aid.

Notes on CE mark

The devices comply with the regulations of the following European directive:

89/336/EEC
Council Directive on the Harmonization of the Legal Regulations of Member States on Electromagnetic Compatibility (amended by Directives 91/263/EEC, 92/31/EEC and 93/68/EEC).
The EU Declaration of Conformity is kept available for the responsible authorities in accordance with the above-mentioned EU directives at:

Hirschmann Electronics GmbH & Co. KG
Automation and Network Solutions
Stuttgarter Straße 45-51
D-72654 Neckartenzlingen
Germany
Phone (07127) 14-1538

The product can be used in the residential sphere (residential sphere, business and trade sphere and small companies) and in the industrial sphere.
– Interference immunity: EN 61000-6-2:1999
– Radio interference level: EN 55022:1998 Class A

Warning!
This is a Class A device. This equipment may cause radio interference if used in a residential area; in this case it is the operator´s responsibility to take appropriate measures.
The precondition for compliance with EMC limit values is strict adherence to the construction guidelines specified in this description and operating instructions.

FCC Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules.
These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Recycling note:

After usage, this product must be disposed of properly as electronic waste in accordance with the current disposal regulations of your county / state / country.

3.2 Device installation

3.2.1 Controls

DIP switch

With the 3-pin DIP switch in the lower panel of the switch basic module

- You can select the port with the ring port switch for the HIPER-Ring. In the delivery state (OFF position), ports 1 and 2 form the connection for the HIPER-Ring.
  In the ON position, ports 1 and 5 form the connection for the HIPER-Ring. In the ON position, there is also a redundancy of the media module. The ON position offers the option of changing media within the HIPER-Ring.
- The RM functionality (Redundancy Manager) can be switched on or off with the RM switch. State on delivery: In the delivery state (OFF position) the RM function is not active.

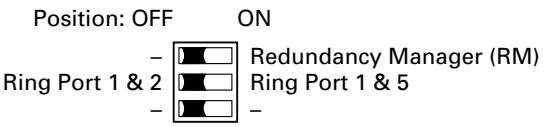


Fig. 16: 3-pin DIP switch

☐ Check whether the switch settings match your requirements.

- **Button**
  With the "SELECT“ button on the switch basic module, you define the display meaning of the LEDs of the media modules (see “Display status” on page 102). By pressing the button, you can continue switching the meaning of the display. The display status LEDs of the switch basic module display the current meaning of the port LEDs of the media modules.

3.2.2 6-pin terminal block

The supply voltage and the signal contact are connected via a 6-pin terminal block with screw locking.

Warning!
The devices MICE are designed for operation with safety extra-low voltage. They may only be connected to the supply voltage connections and to the signal contact with PELV circuits or alternatively SELV circuits with the voltage restrictions in accordance with IEC/EN 60950.

- **Supply voltage**
  The supply voltage can be connected redundantly. Both inputs are decoupled. There is no distributed load. With redundant supply, the transformer supplies the MICE alone with the higher output voltage. The supply voltage is electrically isolated from the housing.

- **Signal contact:**
  The signal contact monitors proper functioning of the MICE, thus enabling remote diagnostics.
  A break in contact is reported via the zero-potential signal contact (relay contact, closed circuit):
  - the failure of at least one of the two supply voltages;
  - a continuous malfunction in the MICE (internal 3.3 VDC voltage;

- the defective link status of at least one port. With the MICE, the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition;
- error during self-test.

In addition the following conditions are reported in RM mode:

- Ring monitoring is not possible, e.g. during software initialization.

Note: With non-redundant supply of the mains voltage, the MICE reports a power failure. You can prevent this message by applying the supply voltage over the two inputs.

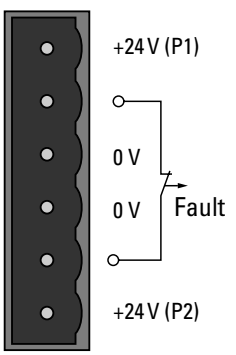


Fig. 17: Pin assignment of the 6-pin terminal block

☐ Pull the terminal block off the MICE and connect the power supply and signal lines.

3.2.3 Assembly

On delivery, the device is ready for operation.
Media modules can be assembled and disassembled during running operation.

☐ Slide the upper snap-in guide of the MICE into the top hat rail and press the guide down against the rail until it snaps into place.

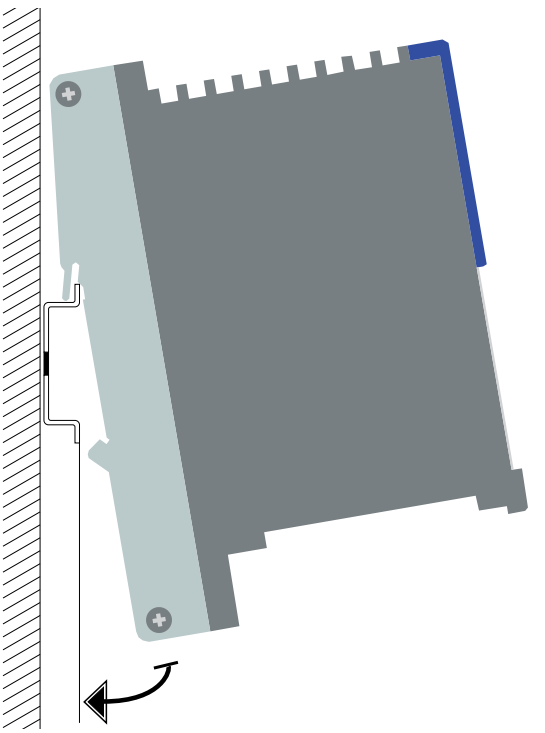


Fig. 18: Assembly

Note: The lower covering panel of the MICE housing is grounded by the tophat rail and, as an option, by the separate ground screw.

Note: The housing must not be opened.

Note: The shielding ground of the industrial connectable twisted pair lines is connected to the lower panel as a conductor.

Media modules

- ☐ To fasten a media module, first remove the protective cap over the plug.
- ☐ Plug the media module onto the plug.
- ☐ Tighten the 4 screws on the corners of the media module.
- ☐ Install the media modules in succession from the left to the right.

MB3 - 2T expansion module

The MB3 - 2T expansion module can be installed while in running operation.

- ☐ On the right side of the MS3124 - 4 switch basic module, loosen the screw at the top and at the bottom (1-3 revolutions).
- ☐ Remove the side cover.
- ☐ If you have not yet done so, mount the MS3124 - 4 switch basic module onto the top-hat rail.
- ☐ Slide the MB3 - 2T expansion module on the top-hat rail toward the MS3124 - 4 switch basic module until the modules plug into each other.
- ☐ On the MS3124 - 4 switch basic module, tighten the screws at the top and at the bottom.

3.2.4 Interfaces

10/100 Mbit/s connection

10/100 Mbit ports (8-pin R45 sockets) make it possible to connect terminal equipment or independent network segments compliant with the IEEE 802.3 100BASE-TX / 10BASE-T standards. These ports support:
– Autonegotiation
– Autopolarity
– 100 Mbit/s halfduplex,
– 100 Mbit/s fullduplex,
– 10 Mbit/s halbduplex,
– 10 Mbit/s fullduplex.
Delivery state: autonegotiation activated except for the HIPER-Ring port: 100 Mbit/s vollduplex.

The socket housings are electrically connected to the lower panel of the module. The pin assignment corresponds to MDI-X.

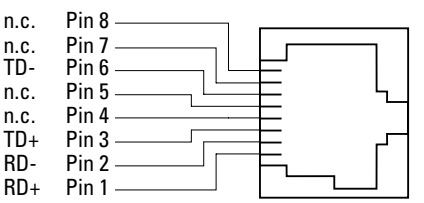


Fig. 19: Pin assignment of a TP/TX interface

10 Mbit/s F/O connection

10 MBit/s F/O ports (ST sockets) make it possible to connect terminal devices or independent network segments compliant with the IEEE 802.3 10BASE-FL standard. These ports support
– full and halfduplex operation

State on delivery: halfduplex.

100 Mbit/s F/O connection

100 MBit/s F/O ports (MTRJ or DSC sockets) make it possible to connect terminal devices or independent network segments compliant with the IEEE 802.3 100BASE-FX standard. These ports support:
– full and halfduplex operation

State on delivery: fullduplex.

V.24 connection (external management)

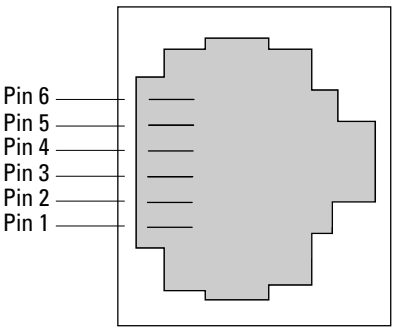
A serial interface is provided on the RJ11 socket (V.24 interface) for the local connection of

- an external management station (VT100 terminal or PC with appropriate terminal emulation). This makes it possible to establish a connection to the user interface UI (see “User Interface” on page 187).
- an AutoConfiguration Adapter ACA 11.

VT-100 Terminal settings:
– Speed: 9,600 Baud
– Data: 8 bit
– Stopbit: 1 bit
– Handshake: off
– Parity: none

The V.24 connection can be activated with the Baud rates 9,600 or 19,200. The setting at system start is 9,600 Baud.

The socket housing is electrically connected to the lower panel of the device.
The signal lines are electrically isolated from the supply voltage (60 V insulation voltage) and the front panel.



Pin-number	V.24-interface
Pin 1	CTS
Pin 2	not connected
Pin 3	TX
Pin 4	GND
Pin 5	RX
Pin 6	RTS

CTS	Clear To Send
RTS	Request To Send
RX	Receive Data
TX	Transmit Data

Fig. 20: Pin assignment of the V24 interface

☐ Install the signal lines and if necessary, the control line and terminal cable.
☐ Attach the ground cable to the ground screw, if additionally required.

3.2.5 Disassembly

☐ In order to remove the MICE from the tophat rail, press the MICE downward and pull it out from under the tophat rail.

3.3 Startup operation

When the supply voltage is connected via the 6-pin terminal, start up the MICE. Lock the terminal block with the side locking screw.

3.4 Basic settings

Although the MICE is designed for ease of use and complies as far as possible with the “plug and play” principle, certain settings are still necessary for correct operation of the management. IP address(es) must be entered when the MICE is installed for the first time.
The MICE offers 4 possibilities to configure IP addresses:

- Configuration via BOOTP (on delivery: on),
- Configuration via DHCP,
- entry via V.24 connection and
- AutoConfiguration Adapter.

BOOTP (bootstrap protocol)

During startup operation the MICE receives its configuration data according to the flowchart "BOOTP process" (see Fig. 21).

For the MICE a BOOTP server should make available the following data :

```
# /etc/bootptab for BOOTP-daemon bootpd
#
# gw -- gateways
# ha -- hardware address
# ht -- hardware type
# ip -- IP address
# sm -- subnet mask
# tc -- template

.global:\
:gw=0.0.0.0:\
:sm=255.255.240.0:

MICE_01:ht=ether-
net:ha=008063086501:ip=149.218.17.83:tc=.global:
MICE_02:ht=ether-
net:ha=008063086502:ip=149.218.17.84:tc=.global:
.
.
```

Lines preceded by a # character are comments.
The lines under ".global:" make the configuration of several devices easier. With the template (tc) you allocate the global configuration data (tc=.global) to each device.
The direct allocation of hardware address and IP address occurs in the device lines (MICE-0...).
☐ Enter one line for each device.
☐ After `ha=` enter the hardware address of this device.
☐ after `ip=` enter the IP address of this device.
Configuration data received from the BOOTP server is saved into the Flash memory.

To enable/disable BOOTP see “IP Configuration” on page 193 and “System data” on page 130.

DHCP (dynamic host configuration protocol)

The DHCP responds similar to the BOOTP and offers in addition the configuration of a DHCP client with a name instead of the MAC address. For the DHCP, this name is known as the "client identifier" in accordance with rfc 2131.
The MICE uses the name entered under `sysName` as the client identifier in the system group of the MIB II (see page 167) . You can enter the system name directly via SNMP, the Web-based management (see “System data” on page 130) or the user interface (see “System parameters” on page 191).

On startup, an MICE receives its configuration data according to flow chart "BOOTP/DHCP process" (see Fig. 21).

The MICE sends its system name to the DHCP server. The DHCP server can then assign an IP address as an alternative to the MAC address by using the system name.
In addition to the IP address, the DHCP server sends
– The tftp server name (if present),
– The name of the configuration file (if present).
The MICE accepts this data as configuration parameters (see “Configure the network” on page 138).
If an IP address was assigned by a DHCP server, it will be permanently saved locally.

The special feature of DHCP in contrast to BOOTP is that the server can only provide the configuration parameters for a certain period of time (“lease”) . When the time period expires (“lease duration”), the DHCP client must attempt to renew the lease or negotiate a new one. A BOOTP-similar response can be set on the server (i.e. the same IP address is always assigned to a particular client using the MAC address), but this requires the explicit configuration of a DHCP server in the network. If this configuration was not performed, a random IP address – whichever one happens to be available – is assigned.

As long as DHCP is activated, MICE attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address.
To activate/deactivate DHCP, see “Configure the network” on page 138.

Note: When using HiVision network management, ensure that DHCP always assigns the original IP address to each MICEs.

Example of a DHCP configuration file::

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 149.218.16.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 149.218.20.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 149.218.17.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 149.218.17.83;
```

```
server-name "149.218.31.11";
filename "/agent/config.dat";
}
```

Lines that start with a ’#’ character are comment lines.
The lines preceeding the individually listed devices refer to settings that apply to all the following .
The line `fixed-address` assigns a permanent IP address to the device.
For further information, please refer to the DHCP server manual.

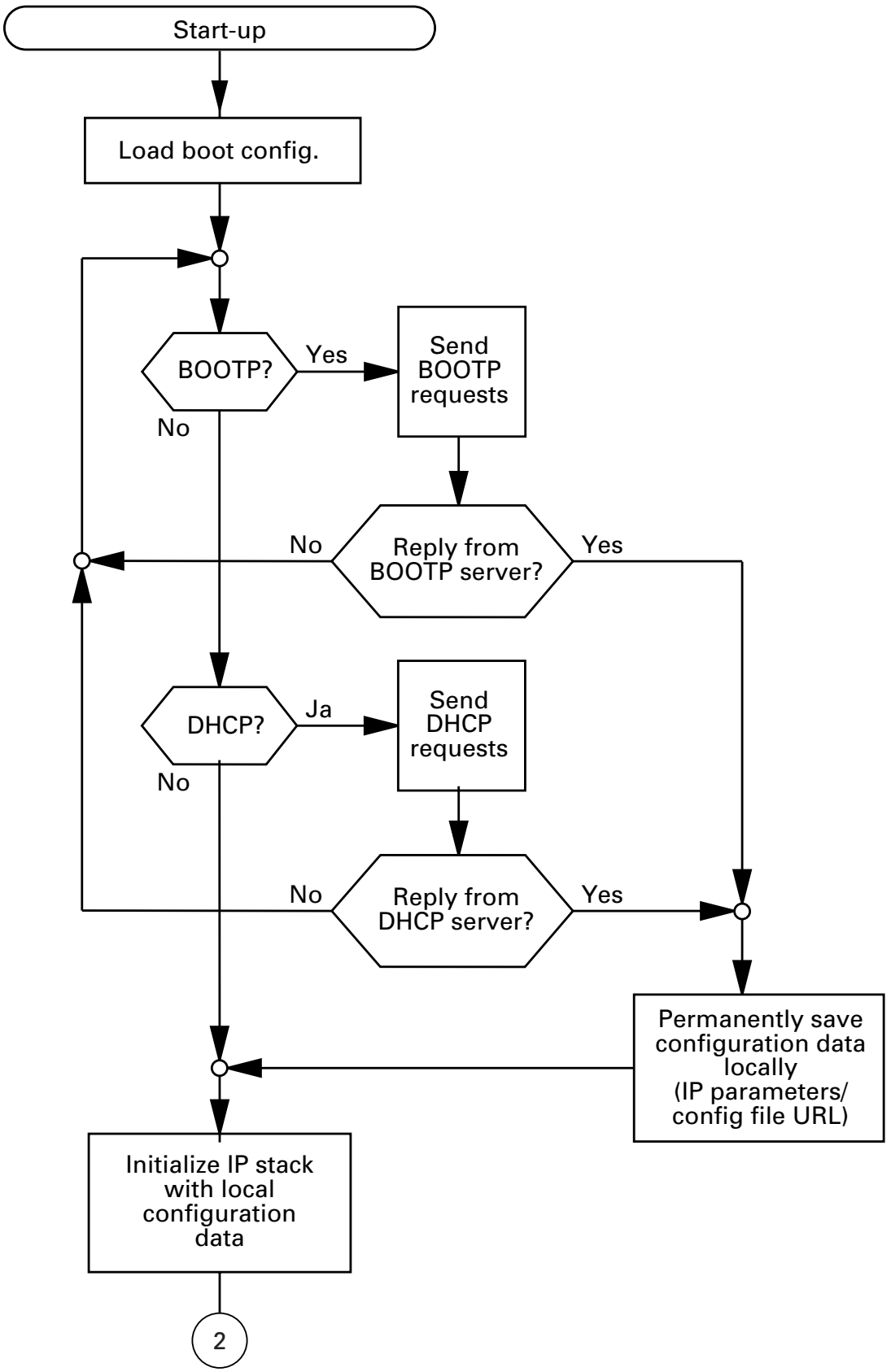


Fig. 21: Flow chart for the BOOTP/DHCP process, part 1

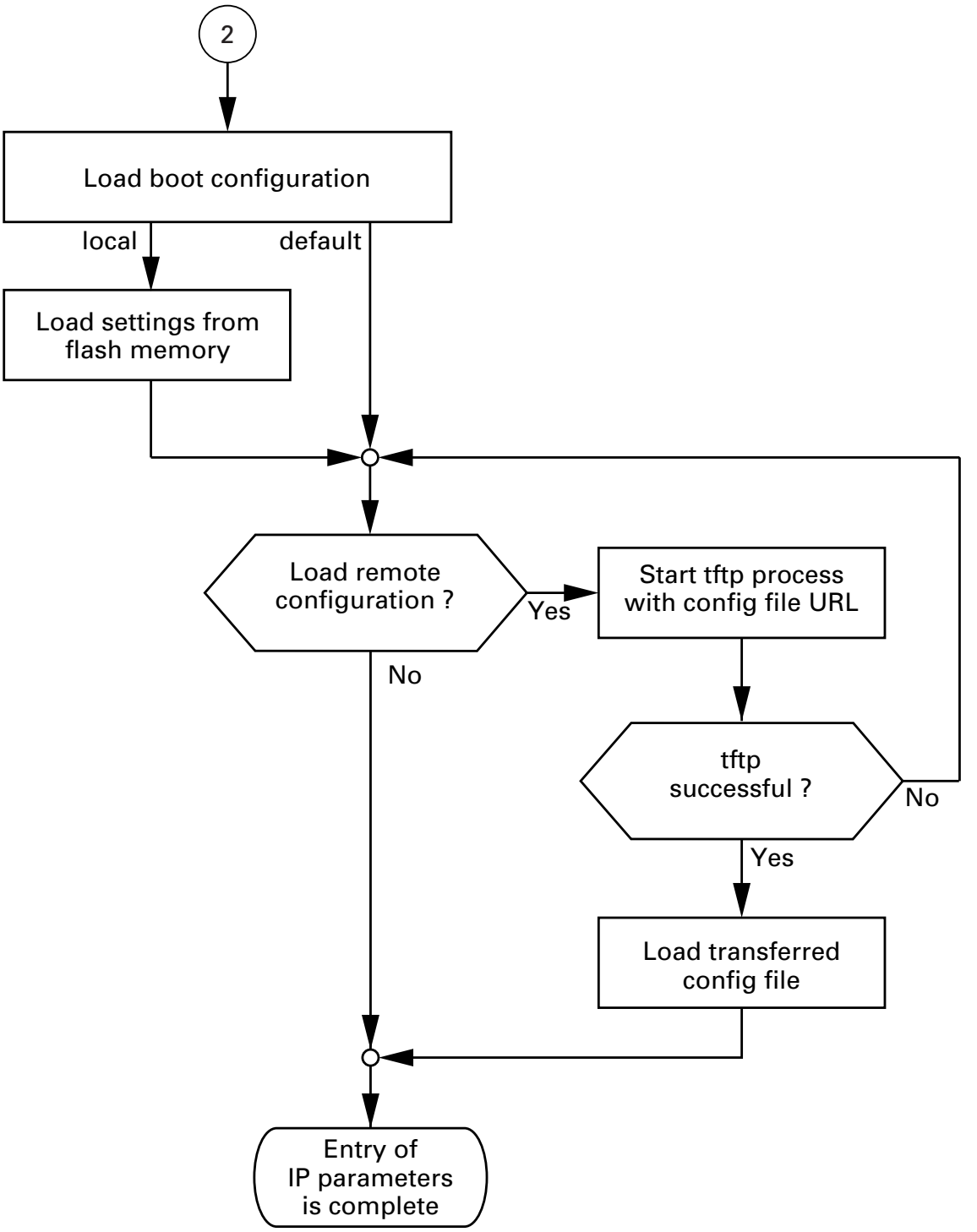


Fig. 22: Flow chart for the BOOTP/DHCP process, part 2

V.24 interface

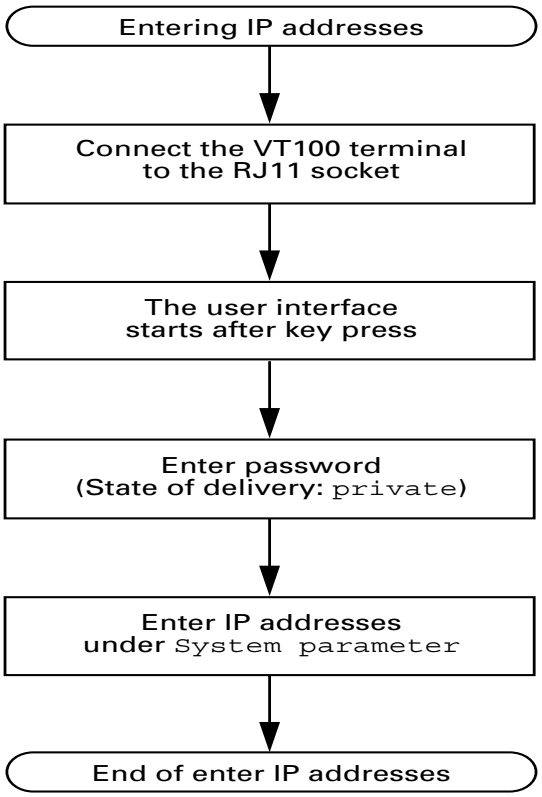


Fig. 23: Flowchart for entering IP addresses

If there is no VT100 terminal available in the vicinity of the installation location, the IP addresses can be entered prior to ultimate installation. A VT100 terminal or suitable emulation (e.g. MS Windows terminal) is required for this purpose.

Note: The installation of MICE is easier if you enter the appropriate IP addresses for each MICE at your workstation. Even if only one MICE is to be installed, it may be more convenient to enter the IP addresses at your own workstation.

The MICE should be labelled to prevent confusion during subsequent installation.

The addresses are stored in a non-volatile memory.

☐ Connect a VT 100 terminal or a PC with terminal emulation to the RJ11 socket (V.24).

Data transfer parameters:

Speed:	9,600 Baud
Data:	8 bit
Parity:	none
Stopbit:	1 bit
Handshake:	off

Note: The transmission rate can be changed in the system monitor (see “3 Change Baudrate” on page 88).

AutoConfiguration Adapter ACA

The ACA is a device for storing the configuration data of a MICE, MICE, or MACH 3000 switch. In the case of a switch failure, the ACA enables a very simple configuration data transfer by means of a substitute switch of the same type.

You can transfer the current switch configuration onto the ACA and the flash memory with "Save local configuration".

You will find further information on operating the ACA in chapters “Configuration” on page 199 and “Defining the start configuration” on page 135.

3.4.1 System configuration

If you do not configure the system via BOOTP, DHCP or the ACA AutoConfiguration Adapter, then perform the configuration via the V.24 interface:

☐ Once the MICE has been installed, start it by connecting the power supply. The operating system is loaded after a key press (see “Starting the User Interface” on page 189).

☐ Enter the password you assigned (pay attention to the style of small and upper case letters) and afterwards press the enter key.

Note: On leaving the factory the password `private` is assigned.

☐ Enter the IP addresses as described in “System parameters” on page 191 and according to the following explanations.

Local IP address
When it leaves the factory, the local IP address of the MICE is 0.0.0.0.

Gateway IP address
This entry is only needed if the MICE and management station/tftp server are located in different subnetworks (see “Example of how the network mask is used” on page 75).
Enter the IP address of the gateway between the subnetwork with the MICE and the path to the management station.
On leaving the factory, the IP address entered is 0.0.0.0.

Network mask
If your network has been divided up into subnetworks and if these are identified with a network mask, then this is to be entered here.
On leaving the factory the subnet mask entered is 0.0.0.0.

3.4.2 IP Address

The IP addresses consist of 4 bytes. These 4 bytes are written in decimal notation, each separated by a dot.

Since 1992, there are five classes of IP addresses defined in RFC 1340. The most frequently used address classes are A, B and C.

Class	Net address	Host address
A	1 Byte	3 Bytes
B	2 Bytes	2 Bytes
C	3 Bytes	1 Byte

Table 1: IP address classification

The network address represents the fixed part of the IP address. It is assigned by the DoD (Department of Defense) Network Information Center.

Fig. 24: Bit notation of the IP address

All IP addresses belong to **Class A** when their first bit is a zero, i.e. the first decimal number is less than 128.
The IP address belongs to **Class B** if the first bit is a one and the second bit is a zero, i.e. the first decimal number is between 128 and 191.
The IP address belongs to **Class C** or **Class D** if the first two bits are a one, i.e. the first decimal number is higher than 191.

Assigning the host address (host id) is the responsibility of the network operator. He alone is responsible for the uniqueness of the IP addresses he assigns.

Network mask

Routers and gateways subdivide large networks into subnetworks. The network mask assigns the individual devices to particular subnetworks.

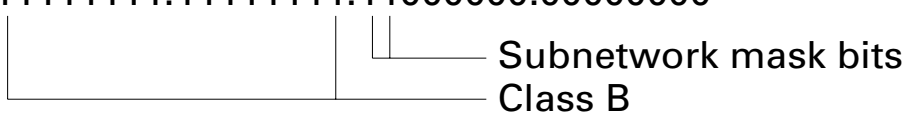
The subdivision of the network into subnetworks is performed in much the same way as IP addresses are divided into classes A to C (net id).

The network part of the IP address is indicated by bits set to one in the mask. The remaining bits, set to zero, indicate the host address.

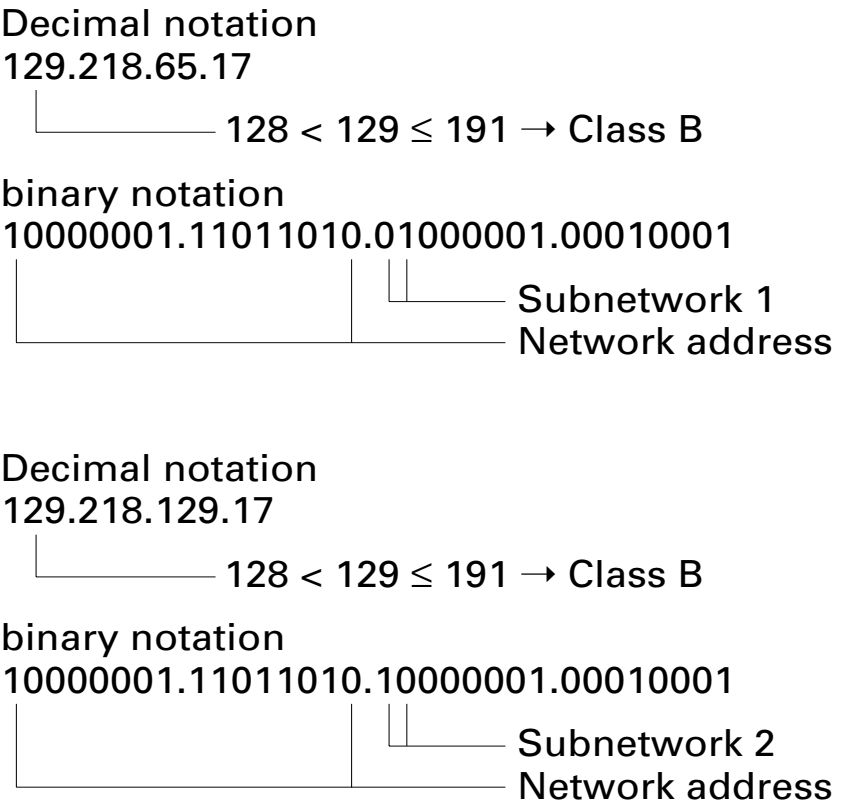
Example of a network mask:

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000



Example of IP addresses which are in different subnetworks when the above subnet mask is applied:


Decimal notation
129.218.65.17
128 < 129 ≤ 191 → Class B
binary notation
10000001.11011010.01000001.00010001
Subnetwork 1
Network address
Decimal notation
129.218.129.17
128 < 129 ≤ 191 → Class B
binary notation
10000001.11011010.10000001.00010001
Subnetwork 2
Network address

Example of how the network mask is used

In a large network it is possible that gateways and routers separate the management agent from its management station. How does addressing work in such a case?

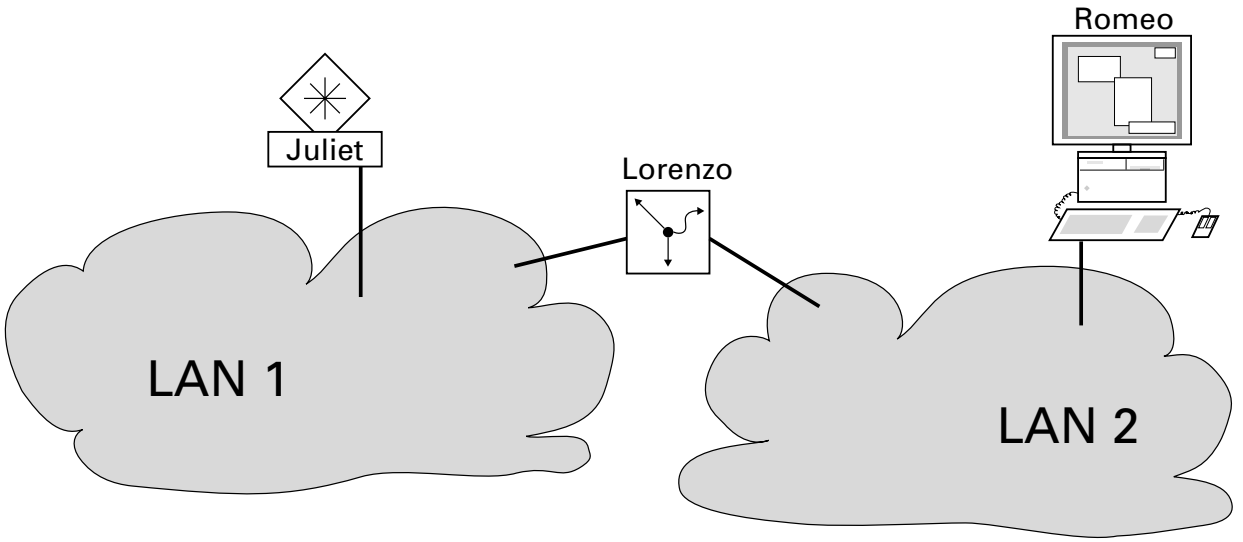


Fig. 25: Management agent that is separated from its management station by a router

The management station “Romeo” wants to send data to the management agent “Juliet”. Romeo knows Juliet's IP address and also knows that the router “Lorenzo” knows the way to Juliet.

Romeo therefore puts his message in an envelope and writes Juliet's IP address on the outside as the destination address. For the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo’s MAC address as the destination and his own MAC address as the source. This process is comparable to going from layer 3 to layer 2 of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox. This is comparable to going from layer 2 to layer 1, i.e. to sending the data packet over the Ethernet.

Lorenzo receives the letter and removes the outer envelope. From the inner envelope he recognizes that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet's MAC address. He writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope, exposing the inner envelope with Romeo's IP address. Opening the letter and reading its contents corresponds to transferring the message to the higher protocol layers of the ISO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo's IP address as destination and her own IP address as source. The question then arises, where should she send the letter, since she did not receive Romeo's MAC address. It was lost when Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable `hmNetGatewayIPAddr` a means of communicating with Romeo. The envelope with the IP addresses is therefore placed in a further envelope with the MAC destination address of Lorenzo.

The letter then travels back to Romeo via Lorenzo the same way the first letter traveled from Romeo to Juliet.

3.5 tftp server for software updates

The switch software is held in the flash memory. The MICE boots the software from the flash memory.

Software updates can be realized via a tftp server. This presupposes that a tftp server has been installed in the connected network and that it is active.

The MICE requires the following information to be able to make a software update from the tftp server:

- Own IP address (permanently entered),
- IP address of tftp server or gateway to tftp server,
- Path in which the software is held on the tftp server.
  (see “Updating” on page 200).

File transfer between MICE and tftp server is handled by way of the **T**rivial **F**ile **T**ransfer **P**rotocol (tftp).

Management station and tftp server may be made up of one or more computers.

Preparation of the tftp server for the MICE software involves the following:

- Setting-up of MICE directories and copying of MICE software
- Setting-up of tftp process

3.5.1 Setting up the tftp process

General prerequisites:

- MICE configured with the IP address of the tftp server/gateway.
- TCP/IP stack with tftp installed on tftp server.

The following section contains information on setting up the tftp process for UNIX systems.

SunOS and HP

☐ First check whether the tftp daemon (background process) is running, i.e. whether the file /etc/inetd.conf contains the following line (see Fig. 26) and whether the status of this process is "`IW`":

SunOS

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd
-s /tftpboot
```

HP

```
tftp dgram udp wait root /usr/etc/in.tftpd tftpd
```

If the process is not in the file, or if the related line is commented out (#), modify /etc/inetd.conf accordingly and then re-initialize the INET daemon. This is done with the command "`kill -1 PID`", where PID is the process ID of inetd.
This re-initialization can be executed automatically by input of the following UNIX commands:

SunOS

```
ps -ax | grep inetd | head -1 | awk -e {print $1} |
kill -1
```

HP

```
/etc/inetd -c
```

You can obtain additional information about the tftpd daemon tftpd with the UNIX command “`man tftpd`”.

Note: the command “`ps`” does not always show the tftp daemon, although it is actually running.

Special steps for HP workstations:

☐ During installation on an HP workstation, enter the user tftp in the file `/etc/passwd`.

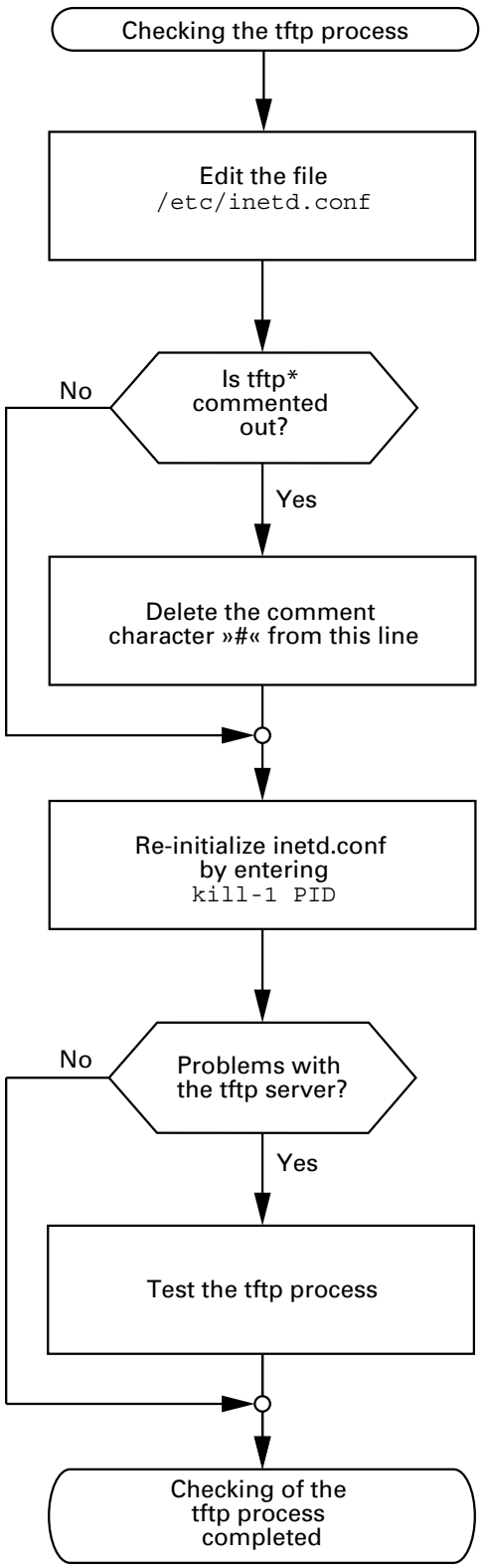
For example:

```
tftp:*:510:20:tftp server:/usr/tftpdir:/bin/false
```

`tftp`	user ID,
`*`	in the password field,
`510`	sample user ID,
`20`	sample group ID,
`tftp server`	rfreely selectable designation,
`/bin/false`	mandatory entry (login shell)

☐ Test the tftp process with e.g.:

```
cd /tftpboot/mice
tftp <tftp-Servername>
get mice/mice.bin
rm rs2.bin
```



e.g
`cd /tftpboot/mice`
`tftp <tftp-Servername>`
`get mice/mice.bin`

Response if the process is running: `Received ...`

`rm mice.bin`

* `tftp dgram udp wait root/usr/etc/in.tftpd in.tftpd /tftpboot`

Fig. 26: Flowchart for setting up tftp server with SunOS and HP

3.5.2 Software access rights

The agent needs read permission to the tftp directory with the MICE software.

Example UNIX tftp server

Once MICE software has been installed, the tftp server should have the following directory structure with the stated access rights:

Filename	Access
rmice.bin	444-r--r--r--

Table 2: Directory structure of the software

`d` = directory; `r` = read; `w` = write; `x` = execute
1st position designates d (directory)
2nd - 4th positions designate access rights of user
5th - 7th positions designate access rights of user groups
8th - 10th positions designate access rights of all others.

3.6 System monitors

The system monitors facilitate the implementation of an

- update of the operating system.

The software update can be implemented via V.24 or tftp.

The V.24 interface of MICE supports the baudrates 9,600, 19,200.

3.6.1 Update of the operating system (System monitor 1)

System monitor 1 facilitates an update of the operating system of the MICE via V.24.

The corresponding screen display shows the following selection:

- 1 Update Operation System
- 2 Start Operation System
- 3 Change Baudrate
- 4 End

Note: System monitor 2 is preferred to update the operating system.

If you boot MICE with 9600 baud, then on the terminal the message “Press <1> to enter Monitor 1” appears.

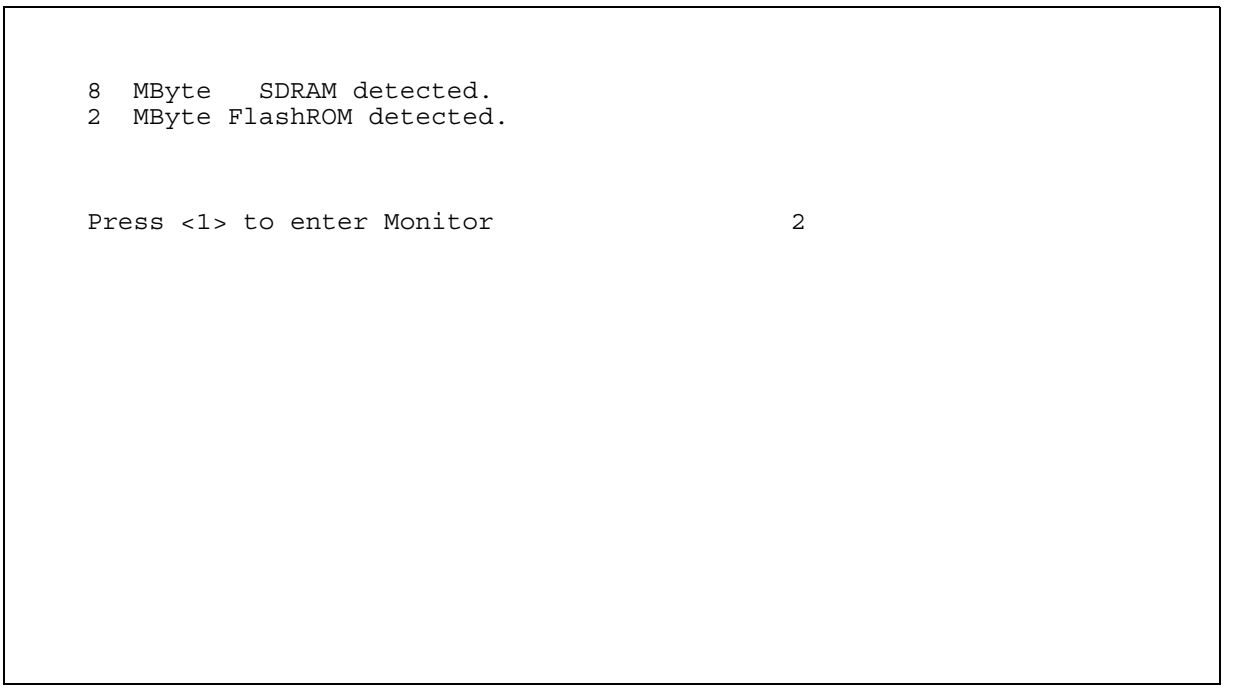


Fig. 27: Screen display during the boot phase

Press the <1> key within one second to start system monitor 1.

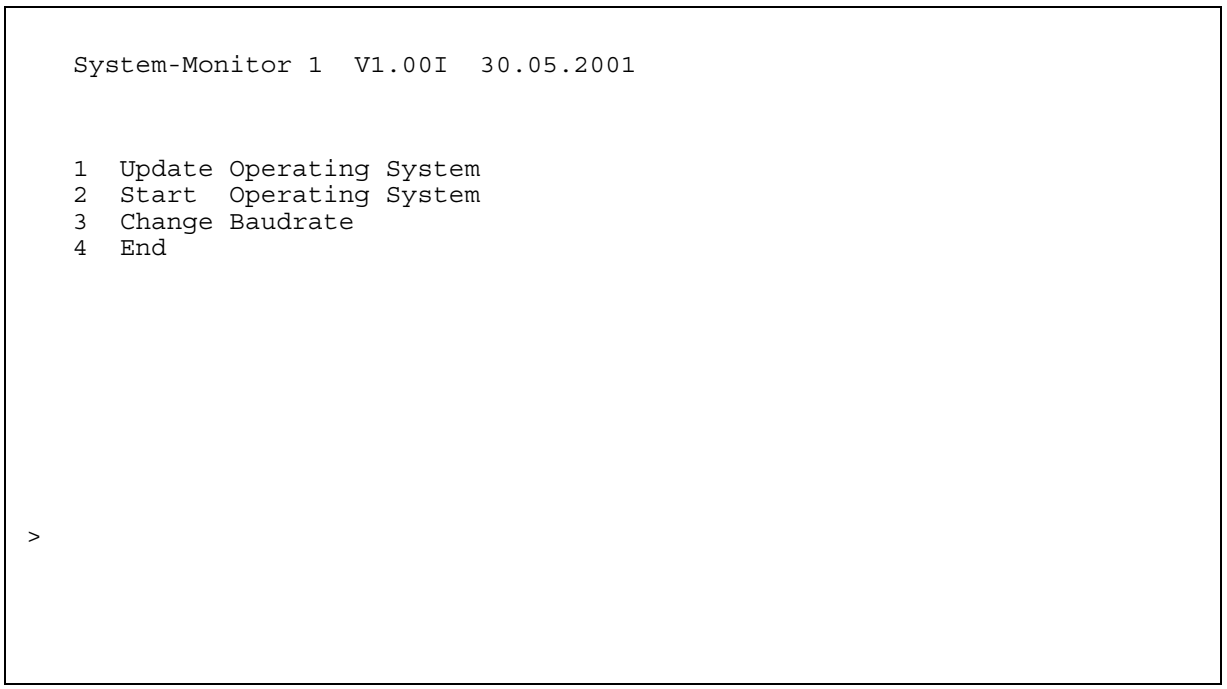


Fig. 28: Screen display “System monitor 1”

1 Update Operation System

This menu allows you to update the operating system.
The following window appears on the screen:

```
         Update Operating System with XMODEM

Maximal buffer size : 2031616 Bytes

 <RETURN> start the XMODEM
 <ESC> end
```

Fig. 29: Screen display “Update operating system”

To leave this screen and return to the main menu of system monitor 1, press the <ESC> key.

Press <RETURN>, to start the update with XMODEM. The following window appears on the screen:

```
Now send file from terminal which supports XMODEM/CRC
The XMODEM starts in 5 seconds
The XMODEM starts in 4 seconds
The XMODEM starts in 3 seconds
The XMODEM starts in 2 seconds
The XMODEM starts in 1 seconds
```

Fig. 30: Screen display when you start an update of the OS

Afterwards enter the name of the path in which the operating system which is to be load is located. Enter the path name via the terminal program, e. g. under Transmission:Binary File. The transmission starts. When the transmission has finished the operating system is restarted.

2 Start Operation System

Enter the figure “2” to start the operating system.
System monitor 1 will be terminated. The operating system will be started with 9,600 baud.

3 Change Baudrate

With this menu you can modify the baudrate.
The following window appears on the screen:

```
   Change baudrate


   1    9600 baud
   2   19200 baud









>
```

Fig. 31: Screen display “Change baudrate”

For an update of your operating system (ref. menu 1) you should choose the maximum speed for the baudrate.
Afterwards adapt the speed of your terminal program to this baudrate.

4 End

This menu terminates system monitor 1.
The following window appears on the screen:

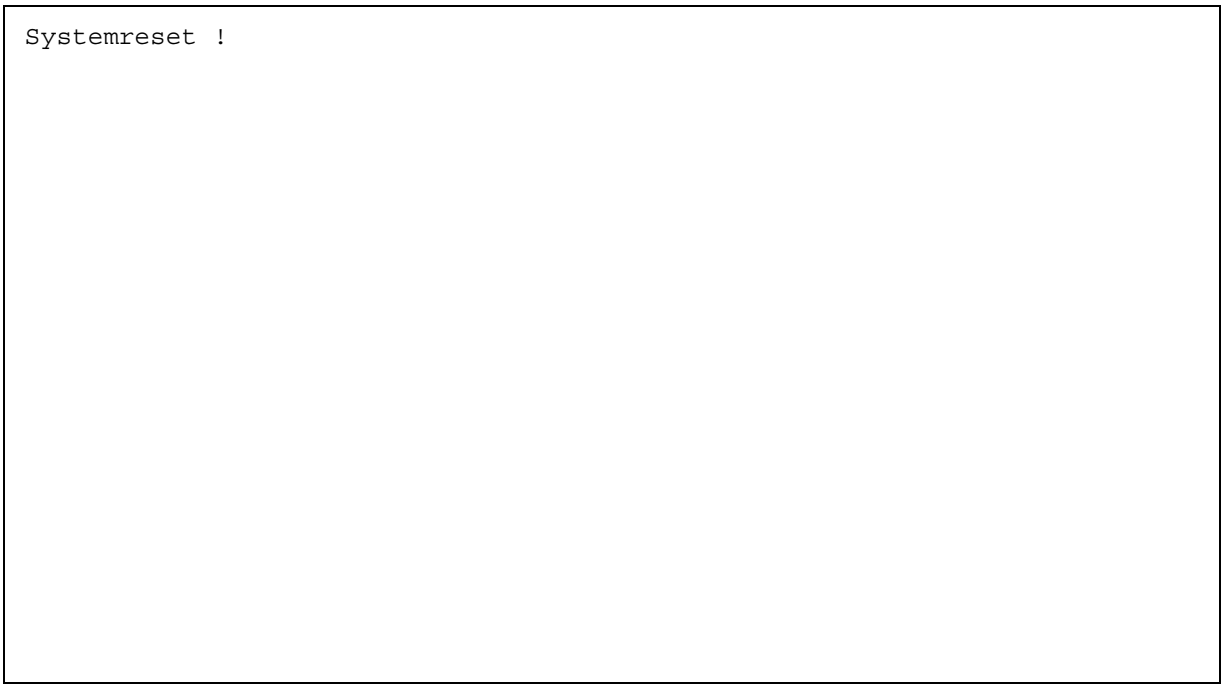


Fig. 32: Screen display “End system monitor 1”

Afterwards execute hardware reset.

3.6.2 Software update (System monitor 2)

System monitor 2 facilitates an update of the MICE operation system via V.24 as well as via tftp.
The corresponding screen display shows the selection

- 1 Software Update V24
- 2 Software Update tftp
- 3 Cancel Automatic Update
- 4 Change Baudrate
- 5 Set Factory Settings
- 6 Reset
- 7 End/Quit

If you boot MICE with 9,600 baud, then the following window appears on the screen:

```
8  MByte   SDRAM detected.
2  MByte FlashROM detected.


Press <2> to enter Monitor                    2
```

Fig. 33: Screen display “Start system monitor 2”

Press the <2> key within three seconds to start system monitor 2.

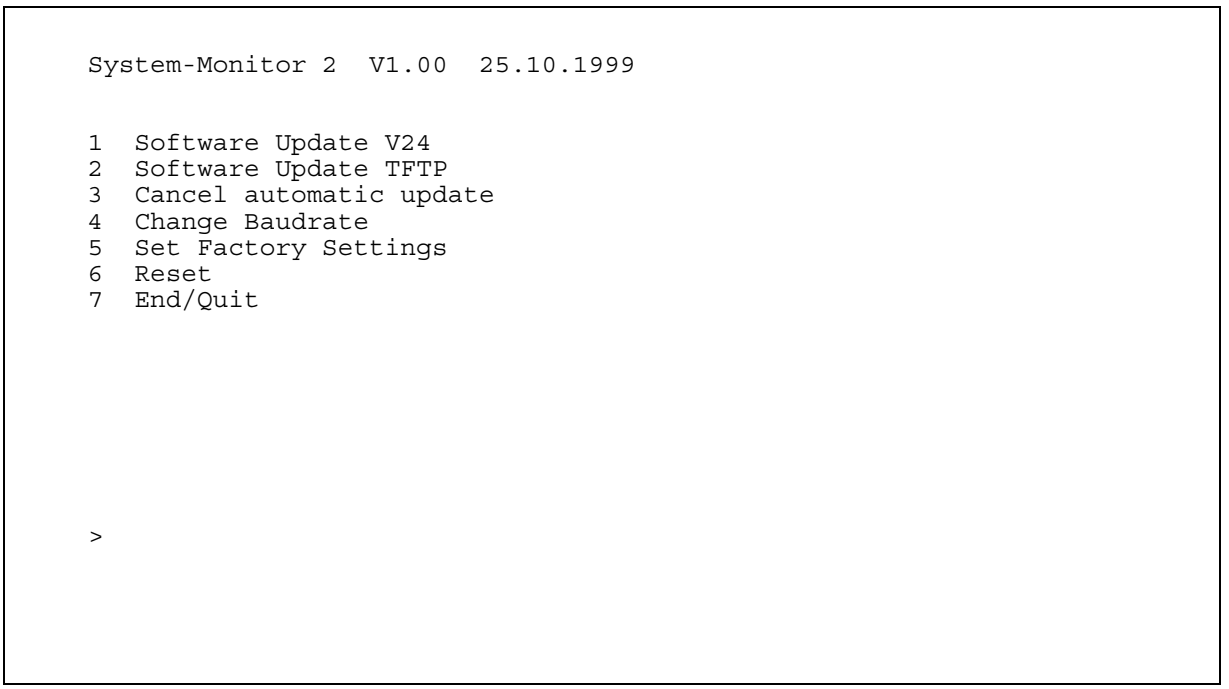


Fig. 34: Screen display “System monitor 2”

1 Software Update V24

This menu executes an update of the operation system in the flash memory of the MICE. The update runs via V.24.

Note: tftp transfer is prefered to update the operation system (see “Updating” on page 200). It is more than three times faster than the fastest V.24 transfer.

The following window appears on the screen:

```
         Update Operating System with XMODEM

Maximal buffer size : 4636149 Bytes

 <RETURN> start the XMODEM
 <ESC> end
```

Fig. 35: Screen display “Update operating system”

To leave this screen and return to the main menu of system monitor 2, press the <ESC> key.

Press <RETURN>, to start the update with XMODEM. The following window appears on the screen:

```
Now send file from terminal which supports XMODEM/CRC
The XMODEM starts in 5 seconds
The XMODEM starts in 4 seconds
The XMODEM starts in 3 seconds
The XMODEM starts in 2 seconds
The XMODEM starts in 1 seconds
```

Fig. 36: Screen display when you start an update of the OS

Afterwards enter the name of the path in which the operating system which is to be load is located. Enter the path name via the terminal program, e. g. under Transmission:Binary File. The transmission starts. When the transmission has finished the operating system is restarted.

2 Software Update tftp

This menu executes an update of the operation system in the flash memory of the MICE. The update runs via tftp.

3 Cancel Automatic Update

This menu terminates the automatic software update.

4 Change Baudrate

With this menu you can modify the baudrate.

5 Set Factory Setting

With this menu item you can restore the original settings. With the exception of the IP parameters, all SNMP MIB variables are reset to their default values.

6 Reset

The device performs a reset.

7 End/Quit

With this menu item you can terminate the system monitor 2.
The management software is started.

4 Functions

The devices of the Hirschmann INDUSTRIAL ETHERNET Rail Switch RS2 family contain a wide variety of functions:

- Frame switching
- GMRP
- Display indicators
- Redundancy
- Management
- SNMP traps

4.1 Hardware functions

4.1.1 Diagnostics

When restarting, the MICE performs a hardware self-test.
During operation, an integrated watchdog (monitoring unit) monitors the function of the software.

4.1.2 Autonegotiation

Autonegotiation is a procedure in which the switch automatically selects the operating mode of its 10/100 RJ-45 ports. When a connection is set up for the first time, the switch detects the speed (10 or 100 Mbit/s) and the transmission mode of the connected network (half duplex or full duplex). The automatic setting of the ports eliminates the need for manual intervention on the part of the user. The autonegotiation function is activated/deactivated by the web management, user interface or SNMP.

Note: If the autonegotiation function is active for only one of both transmission partners, data transmission is halfduplex. The transmission partner determines the transmission rate without autonegotiation.

4.1.3 Autopolarity Exchange

If the receive line pair of a twisted pair cable is incorrectly connected (RD+ and RD- are reversed), polarity is reversed automatically.

4.1.4 Autocrossing

If the autonegotiation function is active, the MICE detects the transmit and receive pairs (MDI, MDI-X). The MICE automatically configures its port for the correct transmit and receive pins. Consequently it does not matter whether you connect devices using a cross-over or straight cable.

4.1.5 Line monitoring

- **Twisted Pair**
  Using regular link-test pulses in accordance with the IEEE 802.3 10/100BASE-TP/TX standard, the MICE monitors the connected TP/TX line segments for short-circuiting or interruptions. The MICE does not send any data to a TP/TX segment from which it does not receive a link-test pulse.

  Note: An unassigned interface is interpreted as a line interruption. The TP/TX line to a deactivated terminal device is also interpreted as a line interruption, since the connected device is unable to send link-test pulses.

- **F/O**
  An MICE monitors the connected fiber optic lines for breaks in accordance with the IEEE 802.3 100BASE-FX standard.

4.1.6 Reset

The MICE is reset by the following events:

- management,
- insufficient level of both input voltages,
- internal supply voltage falls below the threshold value,
- watchdog,
- faulty internal clock.

The following actions are carried out after a reset:

- self-test,
- initialization.

4.2 Display indicators

After applying the operating voltage, the software starts and initializes itself. The MICE then performs a selftest. Various LEDs light up in the process. The process lasts approximately 30 seconds.

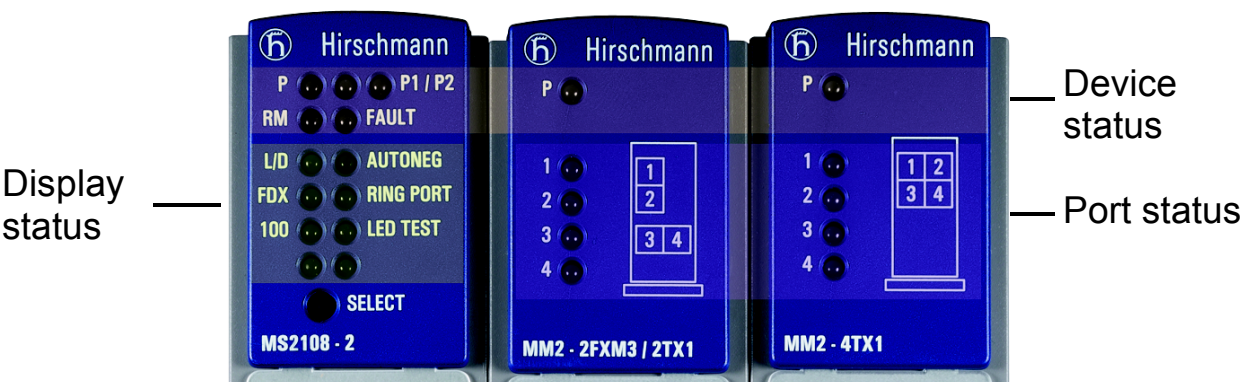


Fig. 37: LED display

4.2.1 Device status

These LEDs provide information about conditions, which affect the operation of the whole MICE.

- **P - Power (Green LED)**
  - – lit: – internal supply voltage applied
  - – not lit: – internal supply voltage is too low

- **P1 – Power 1 (green LED)**
  - – lit: – supply voltage 1 is applied
  - – not lit: – supply voltage 1 is less than 18 V

- **P1 – Power 2 (green LED)**
  – lit: – supply voltage 2 is applied
  – not lit: – supply voltage 2 is less than 18 V

- **RM – Redundancy Manager (green/yellow LED)**
  – lit green: – RM function active, redundant port not active
  – lit yellow: – RM function active, redundant port active
  – not lit: – RM function not active

- **FAULT – Error (Red LED)**
  – lit: – The signal contact is open, i.e. it reports an error.
  – not lit: – The signal contact is closed, i.e. it does not report an error.

4.2.2 Display status

Each media module has one LED per port. The meaning of these port status LEDs depends on the setting on the switch basic module. The display meaning can be set with the "SELECT“ button on the switch basic module.

☐ Press the button approximately 2 seconds to continue switching the meaning of the display. If the button is not pressed for approximately 20 seconds, the display status changes to "L/D.“

- **L/D - data, link status (green LED)**
  – lit green: – The port LEDs of the media modules display the connection status.

FDX - fullduplex (green LED)

– lit green: – The port LEDs of the media modules display the connection type, full or halfduplex.

100 - 10/100 Mbit/s (green LED)

– lit green: – The port LEDs of the media modules indicate the transmission rate.

AUTONEG - autonegotiation (green LED)

– lit green: – The port LEDs of the media modules indicate the port configuration type.

RING PORT - HIPER-Ring port (green LED)

– lit green: – The port LEDs of the media modules indicate the HIPER-Ring assignment.

LED TEST - (green LED)

– lit green: – The status, display status and port status LED test is active.
The status LED "RM“ blinks green/yellow.
The status LED "FAULT“ blinks red.
The display status LEDs blink green.
The port status LEDs of the media modules blink green/yellow.

AutoConfiguration Adapter ACA
Both lower unlabeled LEDs indicate ACA memory operations.
– blink alternatively:
– Error during memory operation.
– LEDs blink synchronously; 2 times per second
– Loading the ACA configuration.
– LEDs blink synchronously; 1 time per second
– Saving the configuration in the ACA.

4.2.3 Port status

These LEDs display port-related information. Set the contents of the information with the button on the switch basic module (see “Display status” on page 102).

1 to 4 – data, link status (green/yellow LED)
– not lit: – no valid connection
– lit green: – valid connection
– blinks green (once a period)
– port is switched to standby (Port 1)
– blinks green (three times a period)
– port is disabled
– blinks yellow: – data reception.

1 to 4 – FDX (green/yellow LED)
– lit green: – fullduplex is active.
– not lit: – halfduplex is active.

1 to 4 – 100 (green/light LED)
– lit green: – 100 Mbit/s is active.
– not lit: – 10 Mbit/s is active.

- **1 to 4 – AUTONEG (green/yellow LED)**
  – lit green: – autonegotiation is active.
  – not lit: – autonegotiation is not active.

- **1 to 4 – RING PORT (green/yellow LED)**
  – lit green: – this port is part of the HIPER-Ring.
  – not lit: – this port is not part of the HIPER-Ring.

- **1 to 4 – LED TEST (green/yellow LED)**
  – blinks green/yellow:– LED test is active.
  – not lit: – LED is defective.

4.3 Frame switching

4.3.1 Store and Forward

All data received by an MICE is stored, and its validity is checked. Invalid and defective data packets (> 1.522 Bytes or CRC errors) as well as fragments (< 64 Bytes) are discarded. Valid data packets are forwarded by an MICE.

4.3.2 Multi-address capability

An MICE learns all the source addresses for a port. Only packets with
- unknown addresses
- these addresses or
- a multi/broadcast address

in the destination address field are sent to this port.

The learned address table can contain up to 4000 addresses. This becomes necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnetworks to an MICE.

4.3.3 Learning addresses

An MICE monitors the age of the learned addresses. Address entries which exceed a certain age (30 seconds, aging time), are deleted by the MICE from its address table.

Note: A reboot deletes the learned address entries.

4.3.4 Prioritization

The MICE supports two priority queues (traffic classes in compliance with IEEE 802.1D). The received data packets are assigned to these classes by the priority of the data packet contained in the VLAN tag.

- Frames with the priority field 0-3 are forwarded with low priority
- Frames with the priority field 4-7 are forwarded with high priority
- All data packets with VLAN tag that contain an unknown target address are transmitted with a lower priority.

This function prevents high priority data traffic being disrupted by other traffic during busy periods. The traffic of lower priority will be discarded when the memory or transmission channel is overloaded.

4.3.5 Tagging

According to the IEEE 802.1 Q standard, the VLAN tag is integrated into the MAC data frame for the VLAN and prioritization functions. The VLAN tag consists of 4 bytes. It is inserted between the source address field and the type field.

With data packets with VLAN tag, the MICE evaluates the 3 Bit priority field within the VLAN tag.

The MAC data frame is transferred unchanged by the MICE.

4.4 Redundancy

4.4.1 Line configuration

The MICE enables the setup of backbones in the line configurations. Cascading takes place via the HIPER-Ring ports.

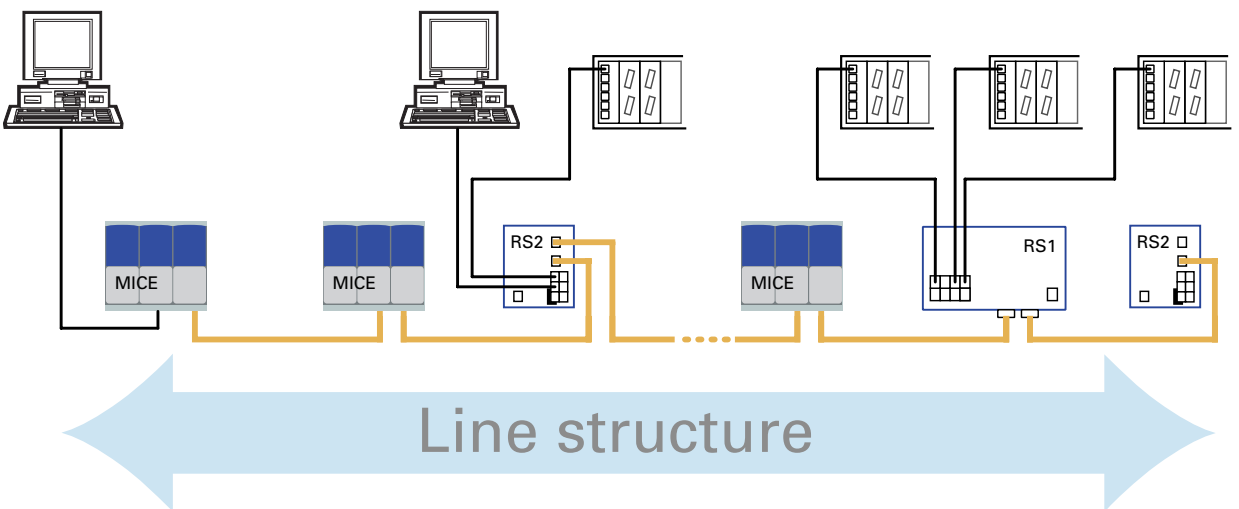


Fig. 38: Line configuration

4.4.2 Redundant ring structure – HIPER-Ring

The two ends of a backbone in a line structure can be closed to form a redundant ring by using the RM function (**R**edundancy **M**anager).

Note: Activate the RM function of a MICE or a MACH 3000, see (“DIP switch” on page 53).

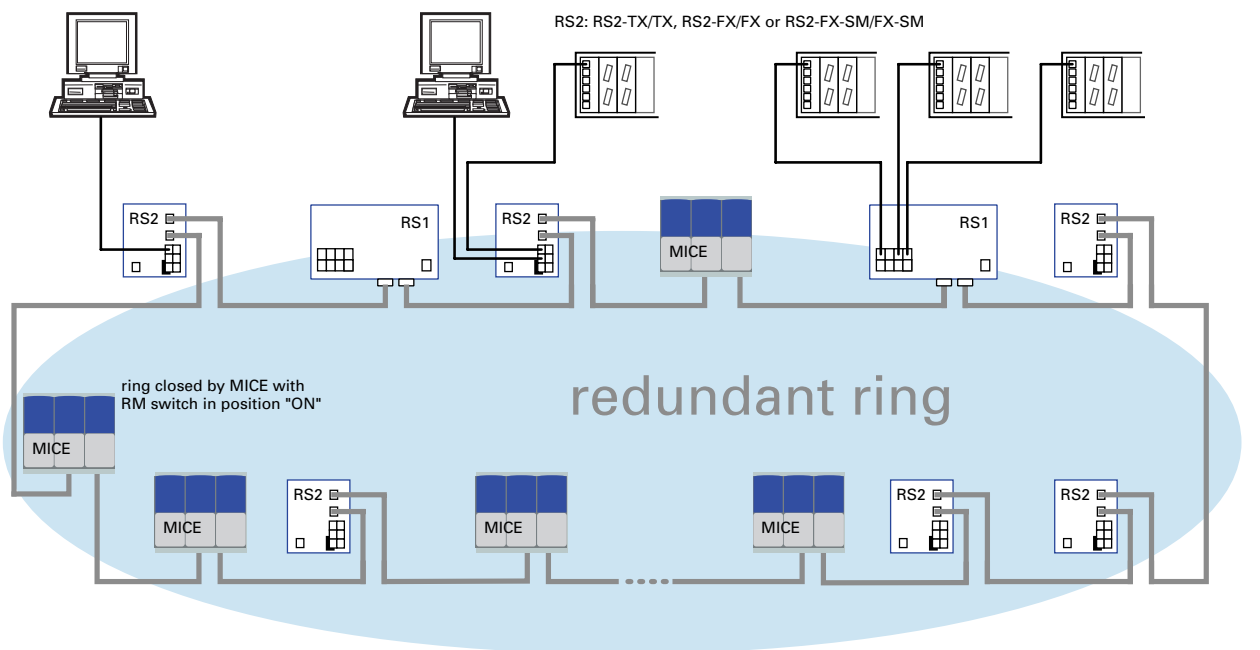


Fig. 39: Redundant ring structure

The MICE is integrated into the ring via the backbone HIPER-Ring ports (ports 1 & 2 or 1 & 5). It is possible to mix the RS1, RS2../.., MACH 3000 and MICE in any combination within the HIPER-Ring. If a line section fails, the ring structure of up to 50 switches transforms back to a line configuration within 0.5 seconds.

Note: The function “HIPER-Ring” requires the following setting for the HIPER-Ring ports:
100 Mbit/s, full duplex and autonegotiation (state on delivery).

4.5 GMRP

The **G**ARP **M**ulticast **R**egistration **P**rotocol (GMRP) describes how multicast information is distributed to other switches. This makes it possible for switches to learn multicast addresses.

Example of a program with GMRP

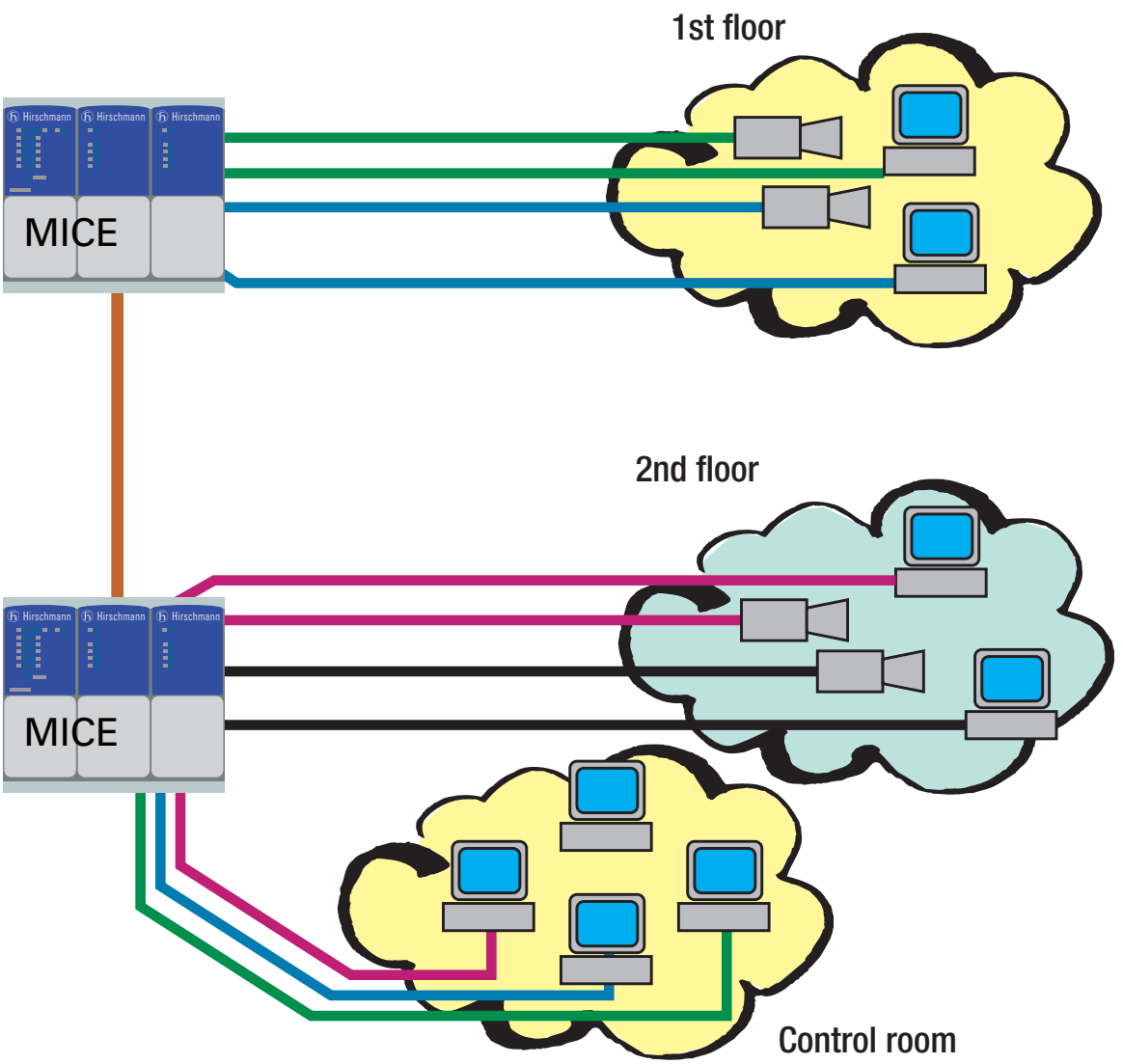


Abb. 40: Example: Video surveillance in machine rooms

The cameras for department store surveillance normally transmit their images to monitor located in the sales room and in the monitoring room.
In a IP transmission, a camera sends its image data with a multicast address over the network.
To prevent the many images from slowing down the entire network, the MICE uses the GMRP to distribute multicast address information. As a result, those images with a multicast address are only distributed to those ports that are connected to the associated monitors for surveillance.

Note: GMRP can be activated by using the HiVision network management (as of release 5.1) or the web-based interface (see “GMRP” on page 152). Proceed by selecting the configuration of the agent in HiVison in the device window. The global setting for the GMRP is in the menu item `Switching General Settings`.
In the port window you will find the setting for this port under `Configuration:GMRP`.

On delivery, GMRP is deactivated at all ports.

Devices that do not support GMRP can be integrated into the multicast adressing scheme by means of a static filter address entry on the connector port.

The multicast tree is set up within 5 seconds in a network of up to 20 MICEs, after the multicast- address has been entered for the first time at an MICE port.

4.6 Security

4.6.1 Port security

A MICE protects every port from unauthorized access. The following functions are available for monitoring every individual port:

- Who has access to this port?
  The MICE recognizes 2 classes of access control:
  - Every: no access restriction
  - User: only an assigned user has access
- What should happen after an unauthorized access attempt?
  The MICE can respond in three selectable ways to an unauthorized access attempt:
  - non: no response
  - trapOnly: message by sending a trap
  - portDisable: message by sending a trap and disabling a port

The settings for port security are made via web-based management “Setting port security” on page 159 or HiVision network management. Proceed by selecting the agent icon `Security` in the device window with the right mouse button. In the agent window that then appears, you will find the table with the respective MIB variables under `Port Security`.

4.6.2 SNMP

The agent communicates with the network management station via the Simple Network Management Protocol. Therefore the network management station uses the HiVision network management software or the web based interface.
Every SNMP packet contains the IP address of the sending computer and the community under which the sender of the packet will access the switch MIB.

The switch receives the SNMP packet and compares the IP address of the sending computer and the community with the entries in the `hmAuthCommTable` and the `hmAuthHostTable` of its MIB. If the community has the appropriate access right, and if the IP address of the sending computer has been entered, then the switch will allow access.

In the delivery state, the switch is accessible via the community ”public” (read only) and ”private” (read and write) from every computer.

To protect your switch from unwanted access:

☐ First define a new community which you can access from your computer with all rights.

Note: make a note of the community name and the associated index. For reasons of security, the community name cannot be read later. Access to the community access, trap destination and trap configuration table is made via the community index.

☐ Treat this community **with discretion** since everyone who knows the community can access the switch MIB with the IP address of your computer.
☐ Limit the access rights of the known communities or delete their entries.

4.6.3 SNMP Traps

If unusual events occur during normal operation of the MICE, they are reported immediately to the management station. This is done by means of so-called **traps**- alarm messages - that bypass the polling procedure ("Polling" means to query the data stations at regular intervals). Traps make it possible to react quickly to critical situations.

Examples for such events are:

- a hardware reset
- changing the basic device configuration
- link down

Traps can be sent to various hosts to increase the transmission reliability for the messages. A trap message consists of a packet that is not acknowledged.
The management agent sends traps to those hosts that are entered in the trap destination table (hmTrapDestTable). The trap destination table can be configured with the web-based management or the management station via SNMP.

SNMP trap listing

All possible traps that can occur are listed in the following table.

authenticationFailure
is sent if a station attempts to access an agent without permission.

coldStart
is sent for a cold and warm start during the boot process after successful management initialization.

hmAutoconfigAdapterTrap
is sent when the ACA 11 AutoConfiguration Adapter is inserted or removed.

linkDown
is sent if the link to a port breaks.

linkUp
is sent if the link to a port is re-established.

hmPowerSupply
is sent if the status of the voltage supply changes.

hmSignallingRelay
is sent if the status of the signal contact changes.

hmStandby
is sent if the operating state of the MICE changes.

risingAlarm
is sent if an alarm input exceeds the upper threshold.

fallingAlarm
is sent if an alarm input falls below the lower threshold.

hmPortSecurityTrap
is sent, if a MAC address is detected at the port that does not correspond to the current settings of:
– `hmPortSecPermission` and
– `hmPorSecAction` set either to `trapOnly` (2) or `portDisable` (3).

hmModuleMapChange
is sent, if the hardware configuration has changed.

hmRingRedReconfig
is sent, if the redundant ring mechanism has switched over.

4.6.4 SNMP traps when booting

The trap ColdStart is sent during every boot procedure.

5 Web-based management

The MICE supports both SNMP management and Web-based management and can thus offer

- extensive diagnostic and configuration functions for fast startup and
- extensive network and device information.

The MICE supports the TCP/IP protocol family.

The user-friendly web-based interface gives you the option of managing the MICE from any location in the network via a standard browser such as Netscape Navigator/Communicator or Microsoft Internet Explorer.
As a universal access tool, the Web browser uses an applet which communicates with the MICE via the Simple Network Management Protocol (SNMP).
The Web-based interface allows you to graphically configure the MICE.

5.1 Opening the Web-based interface

To open the Web-based interface, you will need a Web browser (a program that can read hypertext), for example Netscape Navigator/Communicator version 4.x or Microsoft Internet Explorer version 5 or higher.

☐ Start your Web browser.

☐ Make sure that you have activated JavaScript in your browser.

☐ Establish the connection, by entering the IP address of the MICE, that you want to administer via the Web-based network management in the address field of the Web browser. Enter the address in the following form:

`http://xxx.xxx.xxx.xxx`

Note: The Web-based interface uses the“Java™ Runtime Environment Version 1.3” plug-in. If it is not yet installed on your computer, it will be installed automatically via the Internet when you start the Web-based interface. This installation is very time consuming.

For Windows NT users: Cancel the installation. Install the plug-in from the enclosed CD-ROM. Proceed by starting the program file `j2re1_3_0-win-i.exe` in the Java directory on the CD-ROM.

The login window will appear on the screen.

Fig. 41: MICE login window

☐ Select the desired language.

☐ The password “public” which you have read permission appears in the password field. If you wish to access the MICE with write permission, then highlight the contents of the password field and overwrite it with the password “private” (state at delivery).
Changing the password protects MICE against unauthorized access.

☐ Click OK.

The Web interface of the MICE appears on the screen.

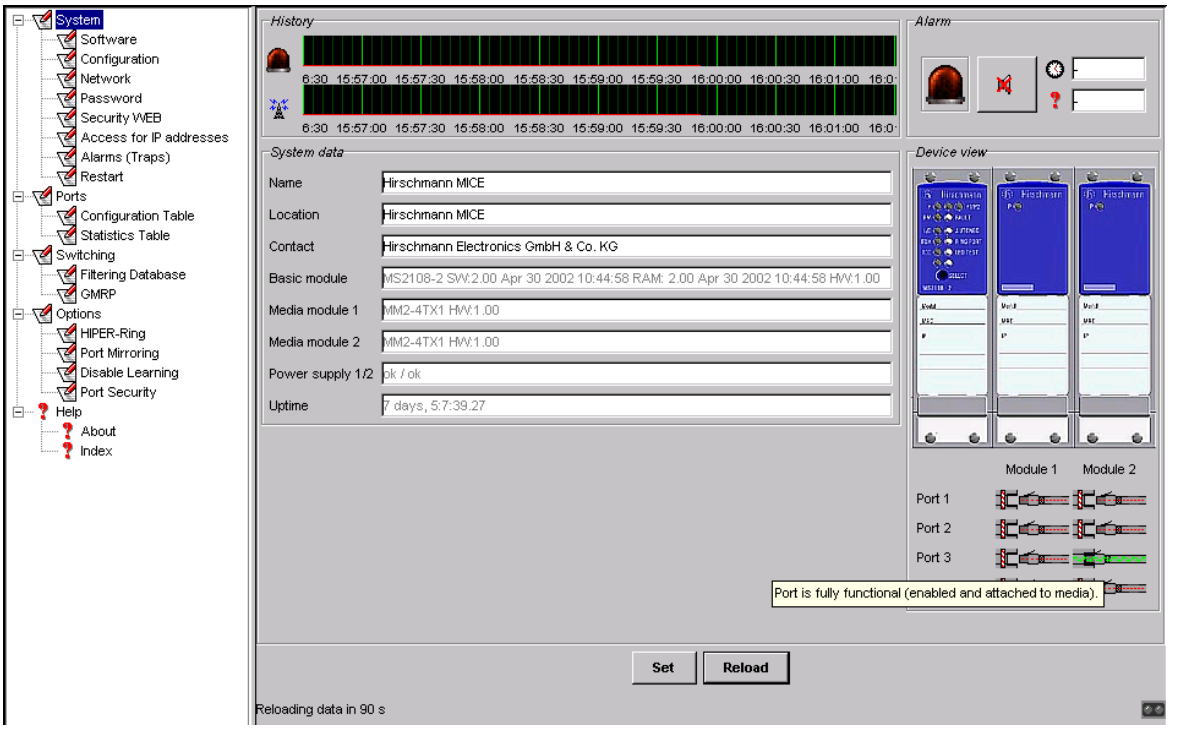


Fig. 42: Web Site of the MICE with bubble help

5.2 Menu tree

The menu section display the menu items. By placing the mouse pointer in the menu section and pressing the right mouse key you can expand the entire menu tree with "Expand all entries“ and you can collapse all entries with "Collapse all entries."

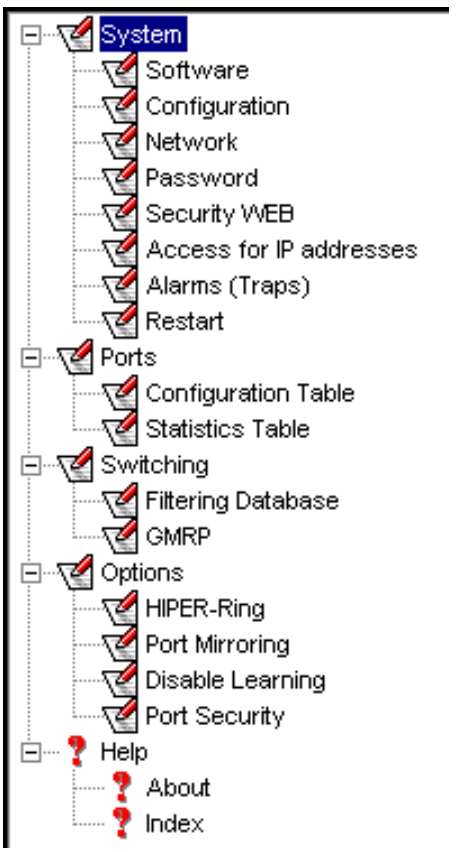


Fig. 43: Menu tree

5.3 System

The system menu contains the dialog boxes and tables used for system configuration:

- Software
- Configuration
- Network
- Password
- Security
- Access for IP addresses
- Alarme (Traps)
- Restart

The information section is divided into:

- History
- Alarm
- System data
- Device view
- Reloading
- Port status

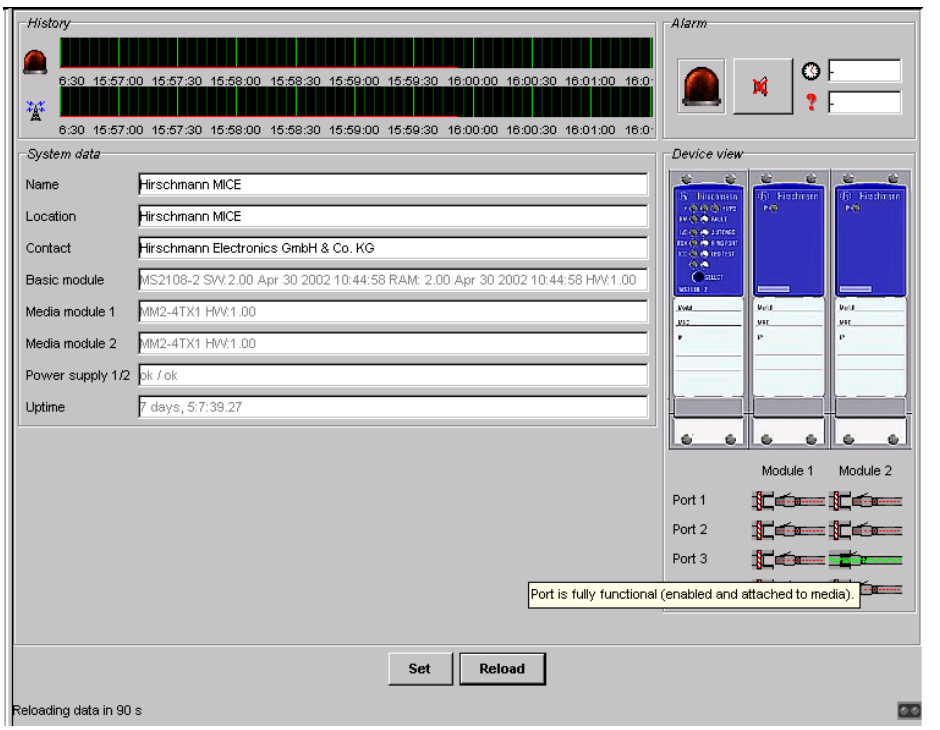


Fig. 44: Information section in the system menu

History

This area of the Web site shows the history of the MICE.
Since the history is maintained by the Web browser applet, the history is available only while the applet is running. The time window extends up to 2 hours.

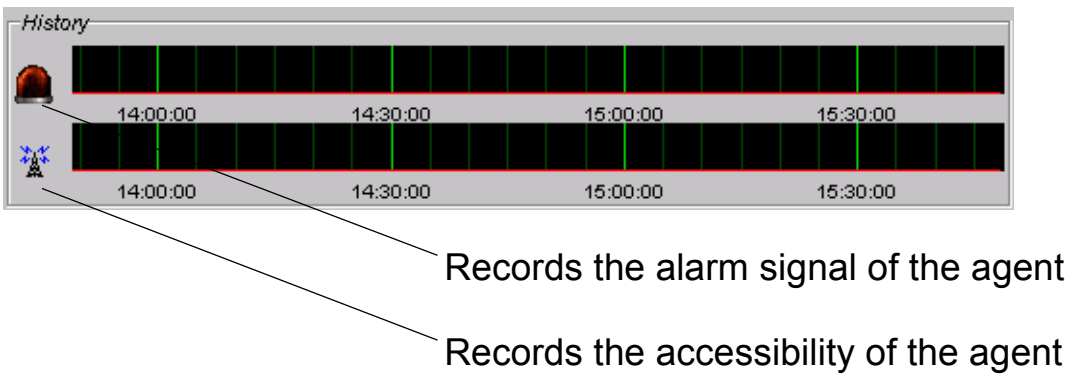


Fig. 45: History display

Alarm

This section of the Web site provides information on the alarm state of the MICE.

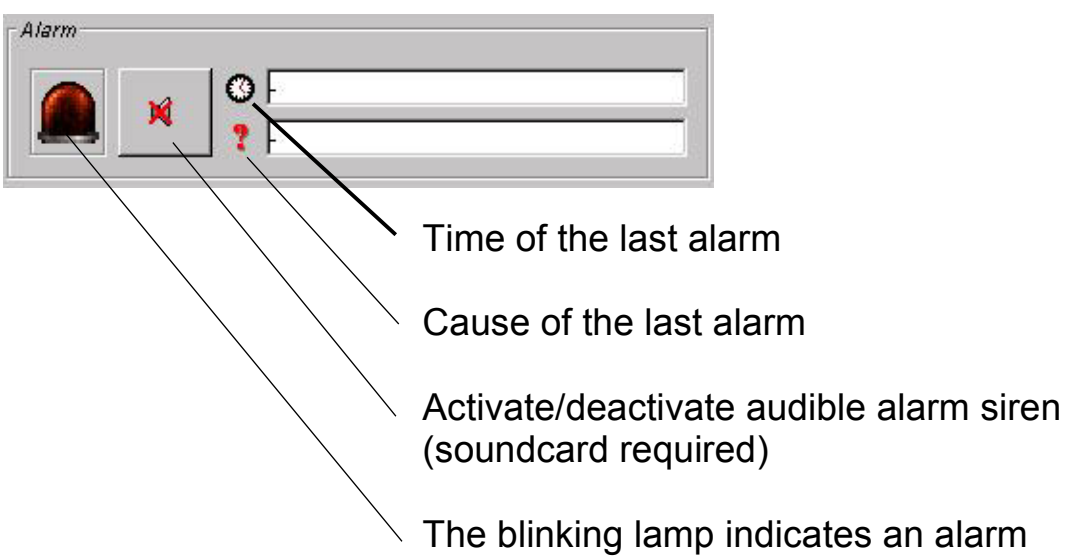
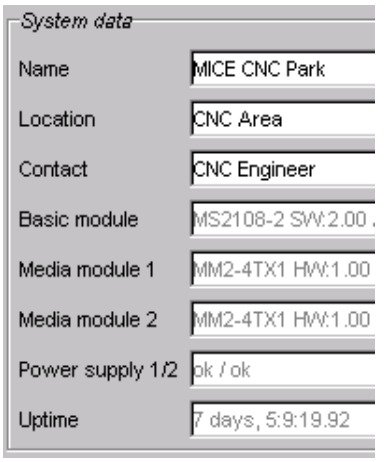


Fig. 46: Alarm display

System data

This area of the Web site displays the system history of the agent. Here you can change,
– the system name,
– the location description and
– the name of the contact person for this switch



– Name of the switch
– Location of this switch
– Contact person for this switch
– Software / hardware version of the basic module
– Software / hardware version of media module 1
– Software / hardware version of media module 1
– Status of the power supply units
– Time that has passed since the switch was last restarted.

Fig. 47: System parameter display

Device view

This area of the Web site displays the switch basic module with the current configuration of media modules. The symbols underneath the device view represent the status of the individual ports.

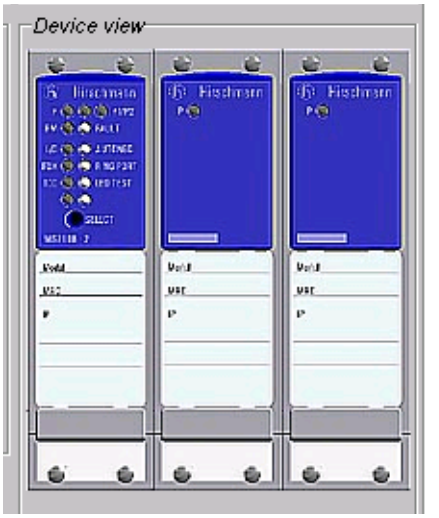
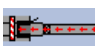
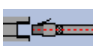


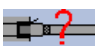
Fig. 48: Device view

Meaning of the symbols:

The port is enabled and the connection is OK.

 The port is locked by management.

 The port is enabled and the connection is interrupted.

 The MICE cannot be reached.

- **Reloading**
  This area of the Web site at the bottom left displays the countdown time until the applet requests the current data of this dialog. Clicking the “Load” button requests the current data of the MICE immediately. The applet polls the current data of the MICE automatically every 100 seconds.

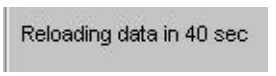


Fig. 49: Time until reload

5.3.1 Updating the software

With this dialog you can carry out a software update of the MICE via tftp or http.

- **tftp Update**
  For a tftp update you need a tftp server on which the software to be loaded is stored. The URL identifies the path to the software stored on the tftp server. The URL is in the format tftp://IP address of the tftp server/path name/file name (e.g. `tftp://149.218.16.5/mice/mice.bin`).
  Click "tftp Update" to load the software from the tftp server to the MICE.

- **http Update**
  For an http update you need access from your computer to the update software.
  If you click "http Update" the MICE opens a second browser window. Here you select the update software and click on "Update" to transfer the software to the MICE.

http Update - 2nd browser window:

☐ Click on `Search` to select the software for the update.

☐ Click on "Update" to transfer the software to the switch.

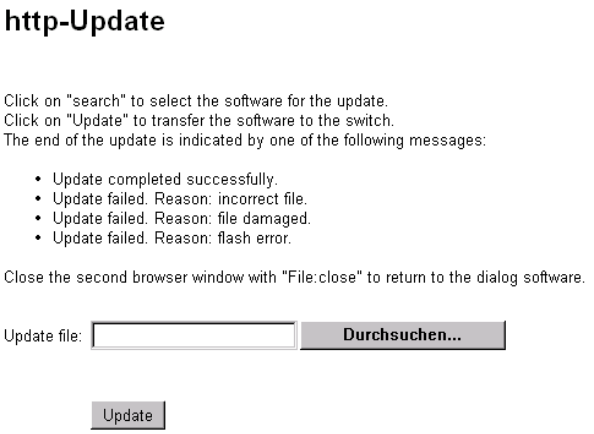


Fig. 50: Dialog software update via http

The end of the update is indicated by one of the following messages:

- ▶ Update completed successfully.
- ▶ Update failed. Reason: incorrect file.
- ▶ Update failed. Reason: file damaged.
- ▶ Update failed. Reason: flash error.

☐ Close this browser window with `"File: close"` to return to the dialog software.

To start the new software after loading, restart the MICE (see dialog “Restarting the switch” on page 145).

Note: You can define what configuration the switch is to be loaded with after restarting in the dialogs “Defining the start configuration” on page 135 and “Configure the network” on page 138 fest

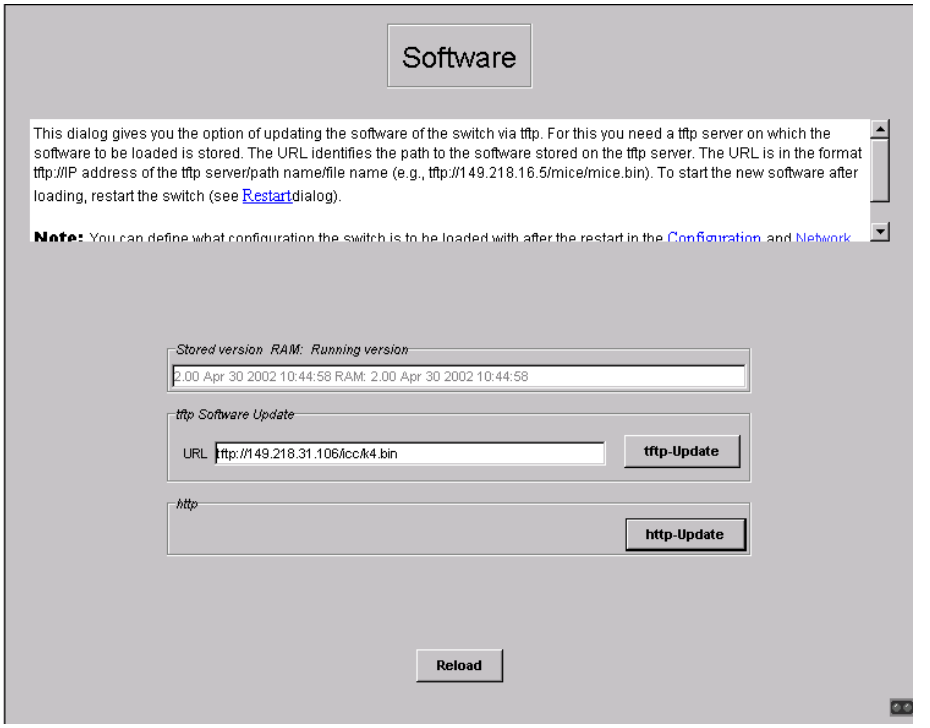


Fig. 51: Dialog Update software

Delete the browser´s cache contents after the software update. After a restart your browser is able to load the new release of the web based interface.

☐ – Netscape Navigator/Communicator:
Close browser and reopen it.
– Microsoft Internet Explorer 5.0:
In Extras:Internetoptionen:Advanced select the topic „Delete Temporary Internet Files when closing the browser“.
Close browser and reopen it.

5.3.2 Defining the start configuration

With this dialog you can:

- Set the configuration with which the system is loaded when restarting. If you select `default`, the parameters are reset to the original delivery state, with the exception of the settings you created in the Software, Configuration and Network dialogs.
- Load a local configuration or one stored under the specified URL.
- Save the current configuration on the device or in a file under the specified URL.
- Enter the URL. The URL identifies the path to the tftp server on which the configuration file is to be stored. The URL is in the form tftp://IP address of the tftp server/path name/file name (e.g. `tftp://149.218.16.5/mice/config.dat`).

  Example to save on a tftp server
  - ☐ Open a new file with any editor.
  - ☐ Save the empty file to the appropriate path of the tftp server, including the file name, e.g. `MICE/MICE_01.cfg`
  - ☐ In line "URL", enter the path of the tftp server, e.g. `tftp://149.218.076.214/MICE/MICE_01.cfg`.

  Note: The configuration file includes all configuration data, including the password. Therefore pay attention to the access rights on the tftp server.
- View the status of the AutoConfiguration Adapter.

Auto Configuration Adapter (ACA)

The ACA is a device for storing the configuration data of a MICE, RS2, or MACH 3000 switch. In the case of a switch failure, the ACA enables a very simple configuration data transfer by means of a substitute switch of the same type.

Storing the current configuration data in the ACA:
You can transfer the current switch configuration onto the ACA and the flash memory with "Save local configuration".

Transferring the configuration data from the ACA:
When you restart, the switch assumes the configuration data of the ACA. and save them permanently into the flash memory.

Status	Meaning
notPresent	No ACA present.
ok	The configuration data from the ACA and the switch are consistent.
removed	The ACA has been removed after rebooting.
notInSync	The configuration data from the ACA and the switch are not consistent.
outOfMemory	The local configuration data is too extensive to be stored on the ACA.
wrongMachine	The configuration data in the ACA comes from another device type.
checksumErr	The configuration data is damaged.

Table 3: ACA status

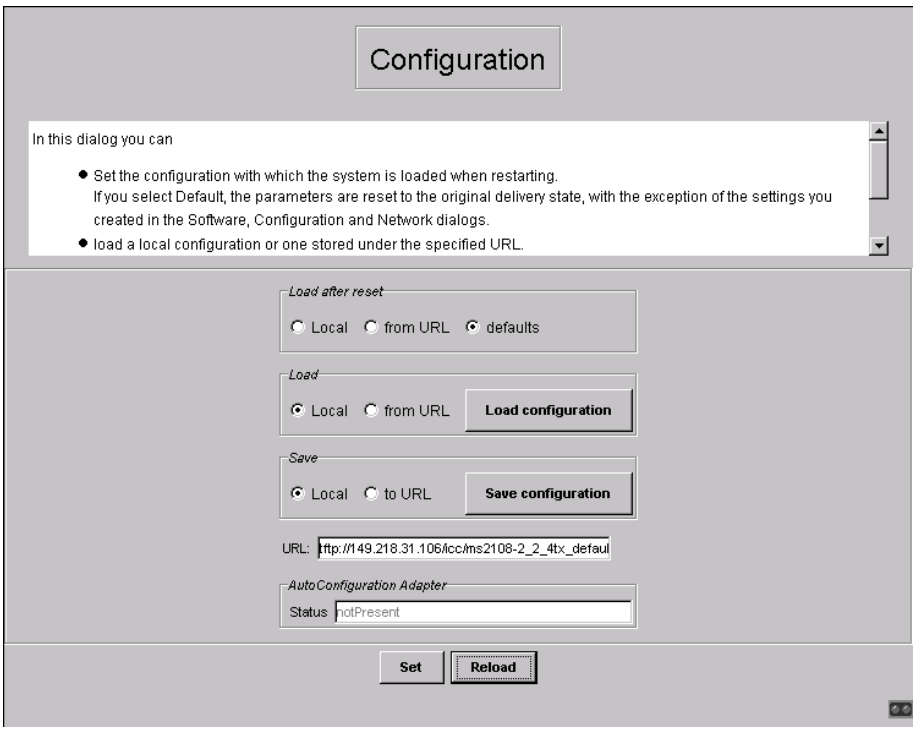


Fig. 52: Dialog Start configuration

5.3.3 Configure the network

With this dialog you define the source from which the switch gets its network parameters after starting, and assign network parameters.

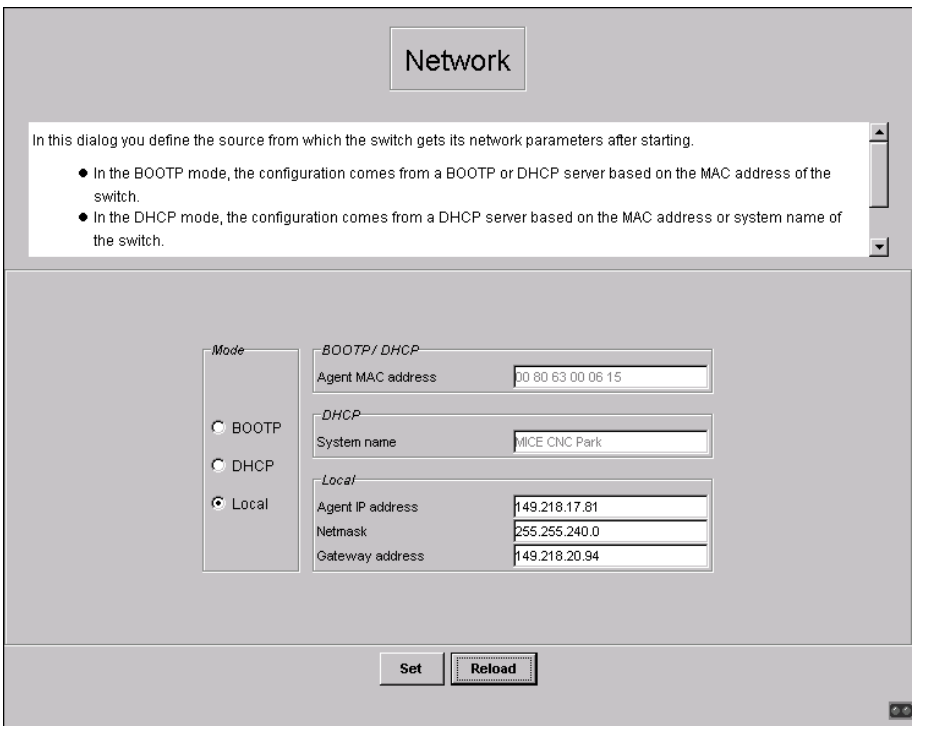


Fig. 53: Dialog Network parameters

☐ Under „Modus“, enter where the MICE is to obtain its IP parameters :

- ► In the BOOTP mode, the configuration comes from a BOOTP or DHCP server on the basis of the MAC address of the switch (see page 63)
- ► In the DHCP mode, the configuration comes from a DHCP server on the basis of the MAC address or the name of the switch (see page 64)
- ► In the local mode the net parameters in the switch memory are used.

☐ Enter the parameters according to the selected mode at the right.

☐ You enter the system name applicable to the DHCP protocol in the “System data” on page 130 dialog, in the "Name" line.

5.3.4 Password

This dialog gives you the option of changing the read and read/write passwords for access to the switch.

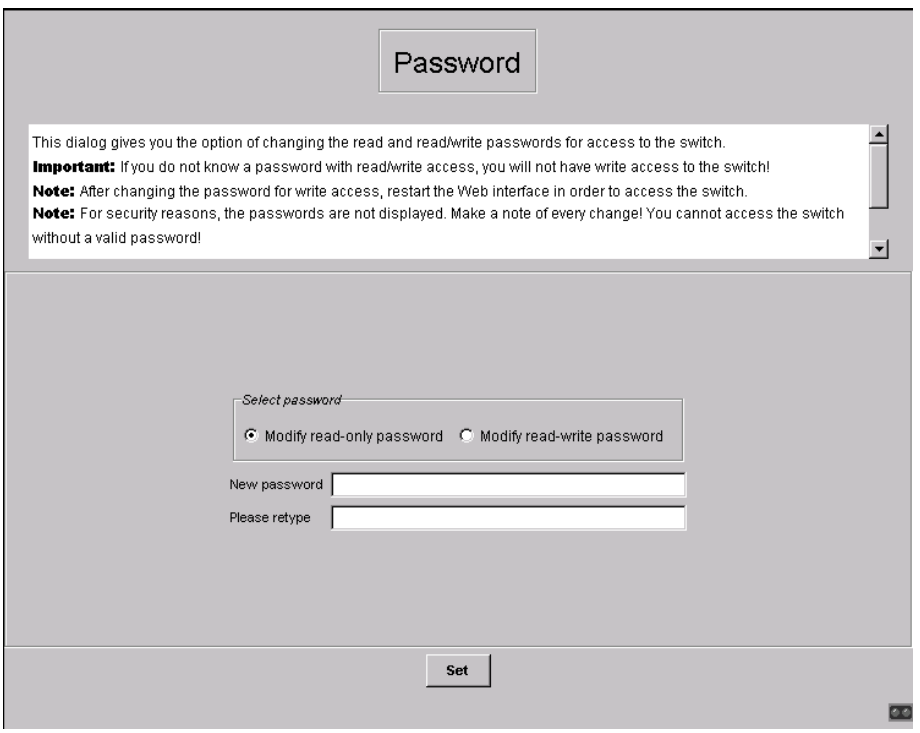


Fig. 54: Dialog Password

Important: If you do not know a password with read/write access, you will not have write access to the switch!

Note: After changing the password for write access, restart the Web interface in order to access the switch.

Note: For security reasons, the passwords are not displayed. Make a note of every change! You cannot access the switch without a valid password!

Access via a Web browser can be blocked with the WEB Access dialog. Access at IP address level is restricted via the Access for IP Addresses dialog.

☐ Enter the new password in the line “New password.”

☐ Repeat the new password in the line “Please re-enter.”

Please note that passwords are case-sensitive.

5.3.5 Security

This dialog allows you to switch off the Web server on the switch. After the Web server has been switched off, the switch can no longer be accessed via a Web browser.

Note: The Web server may be reactivated via the user interface.

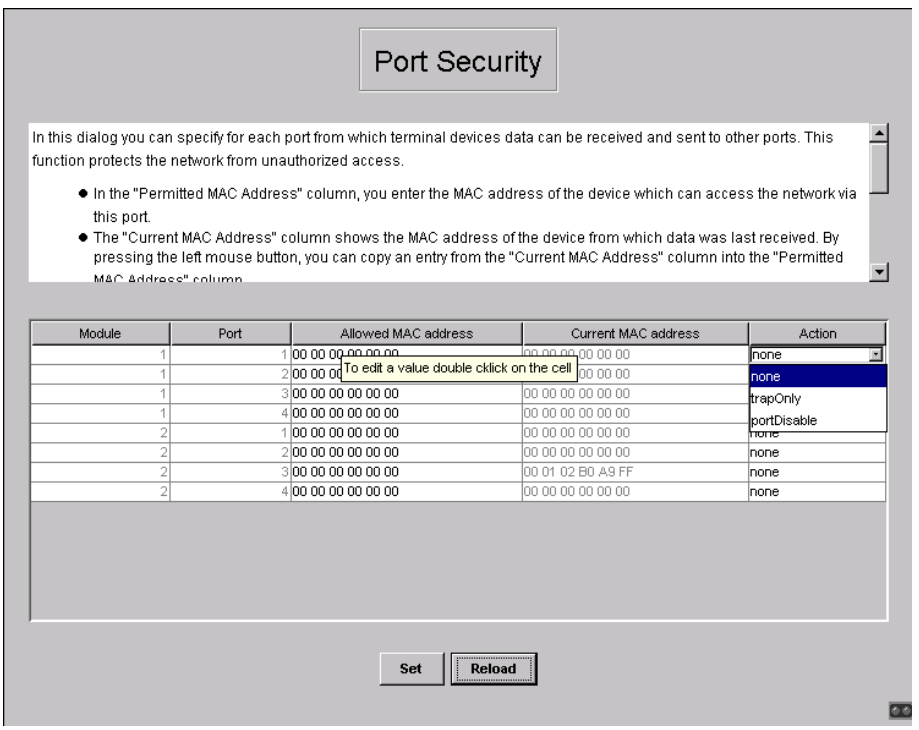


Fig. 55: Dialog Security

5.3.6 Access for IP addresses

This dialog allows you to specify via which IP addresses the switch may be accessed, and what kinds of passwords are to be used.

- In the "Index" column, you enter the current number to which the access restriction applies.
- In the "IP Address" column, you enter the IP address which may access the switch. No entry in this field, or the entry "0.0.0.0", enables access to the switch from computers with any IP address. In this case, the only access protection is the password.
- In the "Name" column, you can enter a name of your choice for the computer with this IP address.
- In the "Password" column, you specify whether this computer can access the switch with the read or with the read/write password.
- In the "State" column, you mark the entries to which access control applies.

Important: If no line is ticked, then there are no access restrictions with respect to the IP addresses!

Important: If you mark one or more lines, make sure that at least one of the lines has a read/write password. In this way you yourself keep the write access to the switch.

Note: Shaded table entries are those carried out by other management systems, such as HiVision, and cannot be changed with the Web-based management system.

Fig. 56: Dialog Access for IP addresses

5.3.7 Configuring traps

This dialog allows you to specify which events trigger an alarm (trap) and to whom these alarms should be sent.

- In the "IP Address" column, enter the IP address of the management station to which the traps should be sent.
- In the "Name" column, you can enter a name for each recipient.
- In the "State" column, you mark the entries which should be taken into account when traps are being sent.

Note: Shaded table entries are those carried out by other management systems, such as HiVision, and cannot be changed from here.

The events which can be selected are:

- Cold Start: The switch has been switched on.
- Link Down: At one port of the switch, the link to the device connected there has been interrupted.
- Link up: At one port of the switch, the link to a device connected there has been established.
- Authentication: The switch has rejected an unauthorized access attempt (see the Access for IP Addresses and Port Security dialogs).
- Port Security: At one port, a data packet has been received from an unauthorized terminal device (see the Port Security dialog).
- Chassis: Encompasses the following events:
  - Power Supply: The status of a supply voltage has changed (see the System dialog).
  - Signaling Relay: The status of the signal contact has changed.
  - Standby: The status of the redundancy manager has changed (see the HIPER-Ring dialog “Configuring the HIPER-RING function” on page 156).
  - ModuleMapChange: A media module has been added or removed.
  - AutoConfigAdapter: The AutoConfiguration Adapter, ACA, has been inserted or removed.

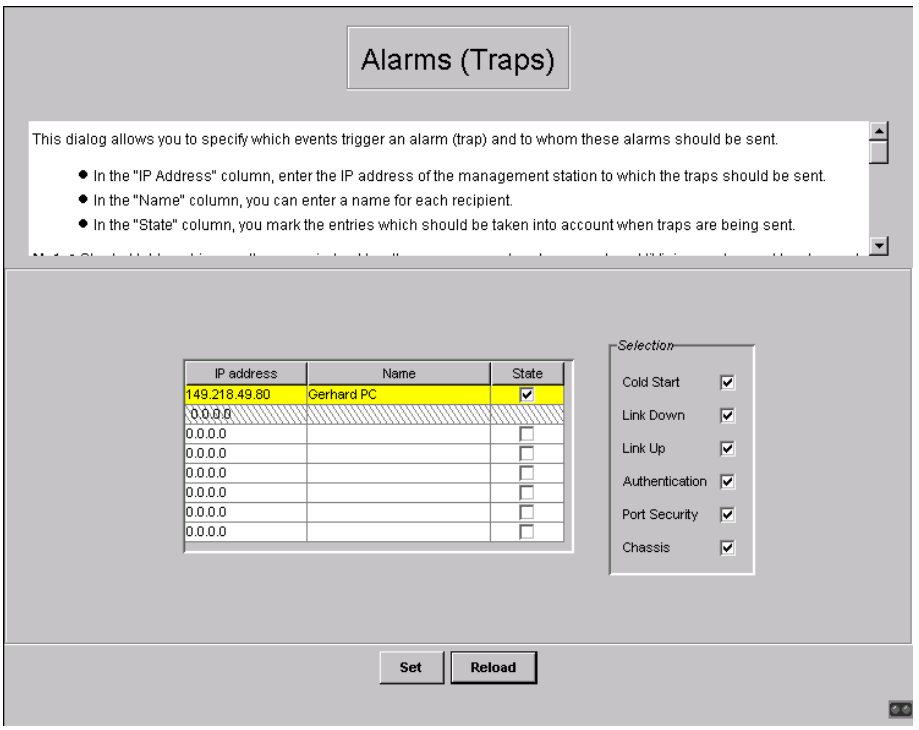


Fig. 57: Dialog Alarms

5.3.8 Restarting the switch

This dialog allows you to restart the switch.

Note: During the restart, the switch temporarily does not transfer any data, and it cannot be accessed via the Web-based interface or other management systems such as HiVision.

5.4 Port

The port menu offers the:

- Port configuration table and the
- Port statistics table.

5.4.1 Port Configuration Table

This table allows you to configure every port of the switch.

- In the "Name" column, you can enter a name for every port.
- In the "Admin Status" column, you can switch on the port by ticking it here.
- In the "Signal Relay mask" column, you can specify that the signal contact is to be opened when a link alarm occurs.
- In the "Autonegotiation" column, you can activate the automatic selection of a port's operating mode by marking the appropriate field. After the autonegotiation has been switched on, it takes a few seconds for the operating mode to be set.
- In the "Manual Configuration" column, you set the operating mode for this port. The choice of operating modes depends on the media module. The possible operating modes are:
  - 10 Mbit/s half-duplex (HDX),
  - 10 Mbit/s full-duplex (FDX),
  - 100Mbit/s HDX and
  - 100Mbit/s FDX.

Note: Note: The active automatic configuration has priority over the manual configuration.

Note: The following settings are required for the ring ports (see “Redundant ring structure – HIPER-Ring” on Page 112):

– 100 MBit/s
– full duplex
– autonegotiation off
– port on.

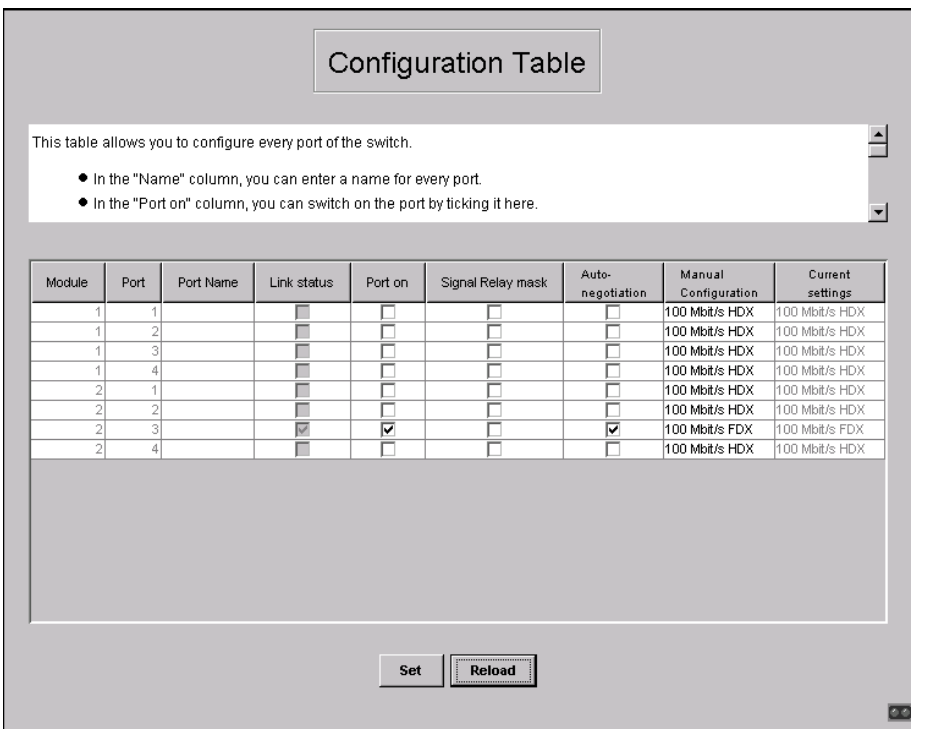
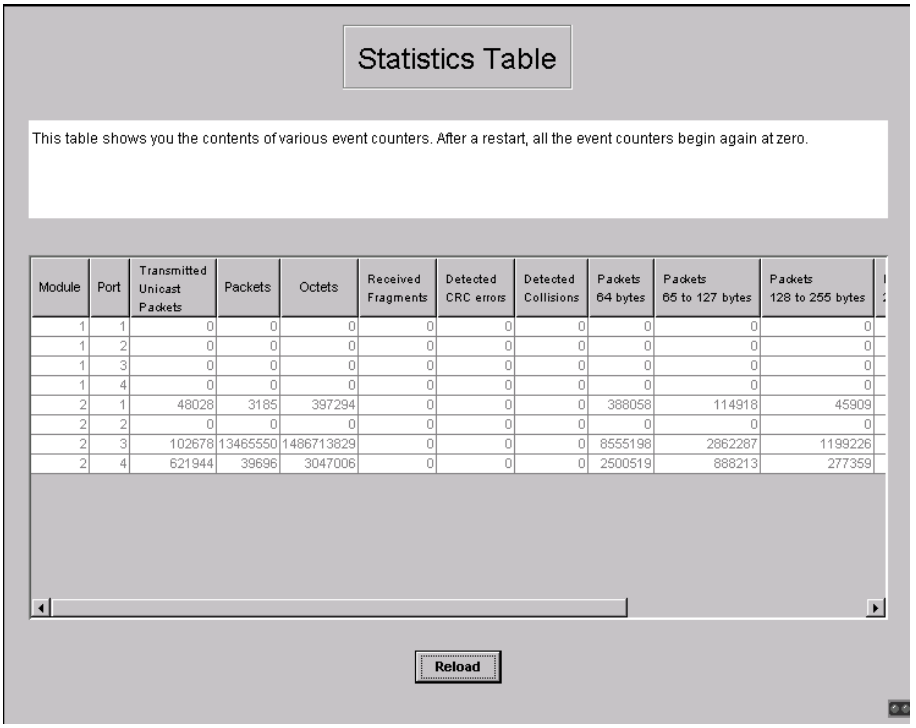


Fig. 58: Dialog Port Configuration Table

5.4.2 Port Statistic Table

This table shows you the contents of various event counters. After a restart, all the event counters begin again at zero.



Module	Port	Transmitted Unicast Packets	Packets	Octets	Received Fragments	Detected CRC errors	Detected Collisions	Packets 64 bytes	Packets 65 to 127 bytes	Packets 128 to 255 bytes
1	1	0	0	0	0	0	0	0	0	0
1	2	0	0	0	0	0	0	0	0	0
1	3	0	0	0	0	0	0	0	0	0
1	4	0	0	0	0	0	0	0	0	0
2	1	48028	3185	397294	0	0	0	388058	114918	45909
2	2	0	0	0	0	0	0	0	0	0
2	3	102678	13465550	1486713829	0	0	0	8555198	2862287	1199226
2	4	621944	39696	3047006	0	0	0	2500519	888213	277359

Fig. 59: Dialog Port Statistic Table

5.5 Switching

The Ports menu includes:

- The port configuration table
- The port statistics table

5.5.1 Filtering Database

This table is used for displaying and editing filters. Each row represents one filter. Filters specify the way in which data packets are sent. They are set automatically by the switch (learned status) or manually. Data packets whose destination addresses are entered in the table are sent from the receiving port to the ports marked in the table. Data packets whose destination addresses are not in the table are sent from the receiving port to all other ports. In the "Create static entry" dialog you can set up new filters. The following status settings are possible:

- Learned: the filter was created automatically by the switch.
- Invalid: with this status you delete a manually created filter.
- Permanent: the filter is stored permanently in the switch or on the URL (see “Defining the start configuration” on page 135).
- DeleteOnReset: the filter is deleted when the switch is reset.
- gmrp: the filter was created by GMRP.
- gmrp/permanent: after the filter has been created by the administrator, GMRP has marked further ports. These ports are deleted when the switch is reset.
- gmrp/deleteOnReset: the filter was created by the adiminstrator and GMRP has marked furhter ports. The filter is deleted when the switch is reset.

In the "Create Filter" dialog (see button below) you can set up new filters.

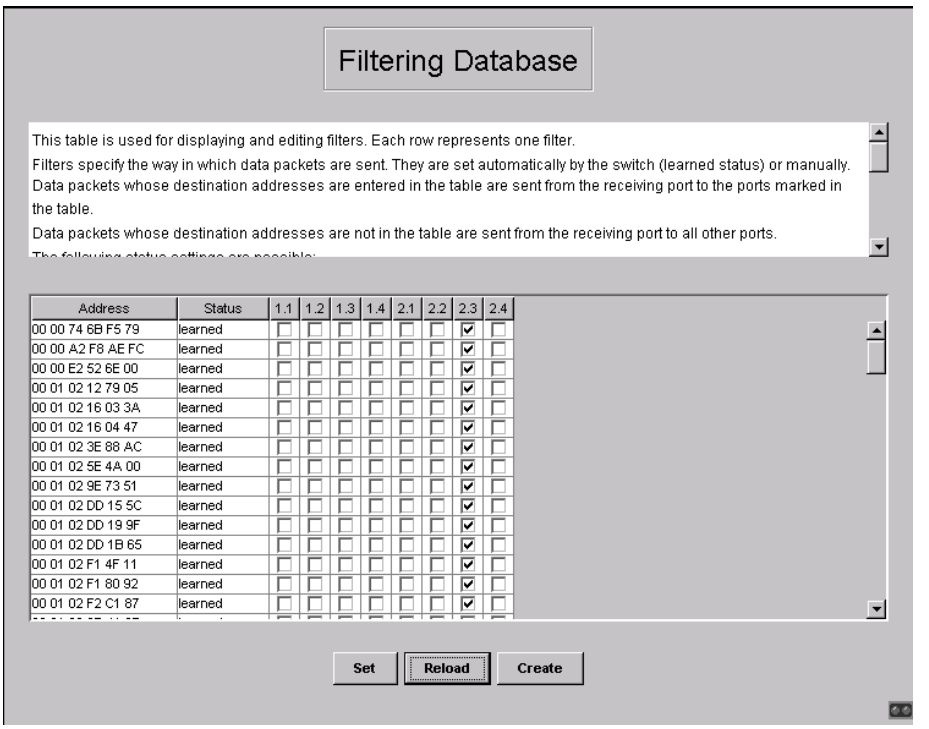


Fig. 60: Dialog Filtering Database

Note: If the redundancy manager is active, it is not possible to enter static unicast addresses.

5.5.2 GMRP

The GARP Multicast Registration Protocol (GMRP) describes the distribution of data packets with a multicast address as the target address. Devices that want to receive data packets with a multicast address as the target address carry out the registration of the multicast address with the aid of the GMRP. For a switch, registration involves entering the multicast address in the filter table. When a multicast address is entered in the filter table, the switch sends this information in a GMRP packet to all the ports. Therefore the connected

switches know that they have to send this multicast address to this switch. The GMRP enables packets with a multicast address in the target address field to be sent to the ports entered. The other ports are not affected by these packets.
Data packets with unregistered multicast addresses are sent to all ports by the switch.

Global GMRP	off
GMRP per port	on
Transmission per port	selective

Table 4: Basic setting of the GMRP

Global GMRP

With the GMRP on/off fields you can switch the GMRP on/off globally for the entire switch.
If the GMRP is switched off, then

- the switch does not generate any GMRP packets,
- it does not evaluate any GMRP packets received, discards them, and
- it sends (streams) received data packets with a multicast address as the target address to all ports.

The switch is transparent for received GMRP packets, regardless of the GMRP setting.

GMRP per port

This table column enables you to switch on/off the GMRP for each port when the global GMRP is switched on. When you switch off the GMRP at a port, no registrations can be made for this port, and GMRP packets cannot be sent out of this port.

Transmission per port

In this table column you find the "GMRP service requirements" of the GMRP standard. They describe the GMRP service requirements of the terminal device on the entire network.

- With the "selective" setting (GMRP default setting: forward all unregistered groups) the switch sends to this port all data packets with a multicast address in the target address field,
  – which is entered in the filter table for this port
  or
  – for which no entry exists in the filter table.
- With the "all" setting (GMRP default setting: forward all groups) the switch sends to this port all data packets with a multicast address in the target address field.

Note: If the switch is connected to a HIPER-Ring, in the case of a ring interruption you can ensure quick reconfiguration of the network for data packets with registered multicast target addresses by:

- switching on the GMRP on the ring ports and globally, and
- selecting the "all" transmission type per port on the ring ports.

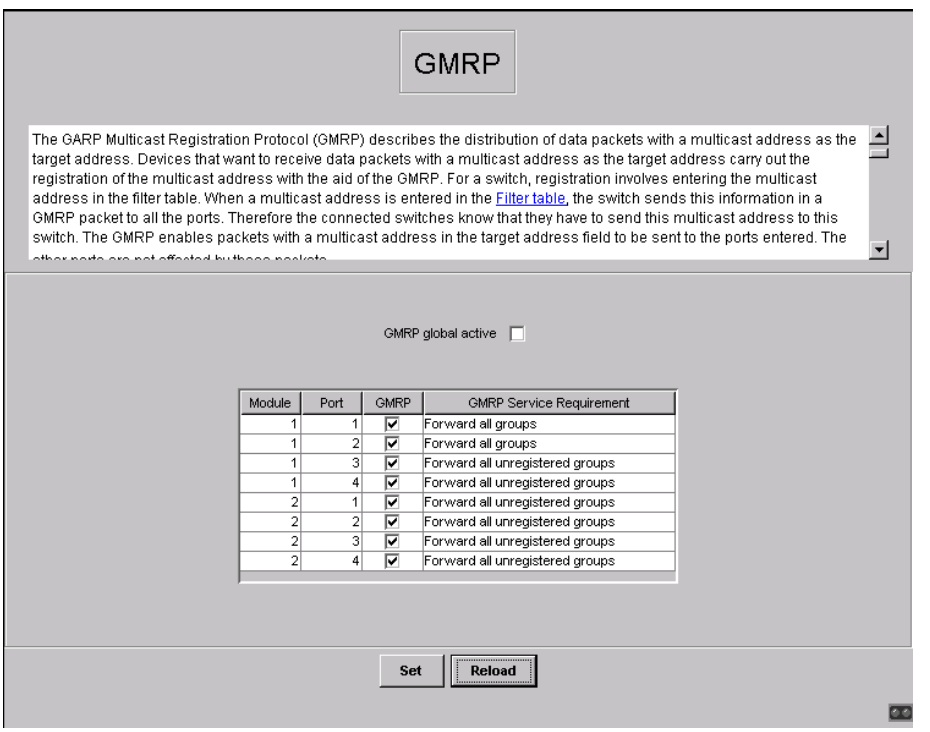


Fig. 61: Dialog GMRP

5.6 Extras

With the Ports menu you can:

- Configure the HIPER-Ring function,
- Set port mirroring,
- Set ports security and
- Disable Learning.

5.6.1 Configuring the HIPER-RING function

This dialog shows you the function of the switch in the HIPER-Ring. The concept of the HIPER-Ring enables the construction of high-availability, ring-shaped network structures. Within such a ring topology, network components supporting the HIPER-Ring are connected with each other via their ring ports. Exactly one redundancy manager assumes control of the ring.
The MICE has DIP switches for selecting the ring ports and for switching the redundancy manager on and off. The status of the redundancy manager is active when the ring is open. This occurs when, for example, a data cable or a network component within the ring is down.

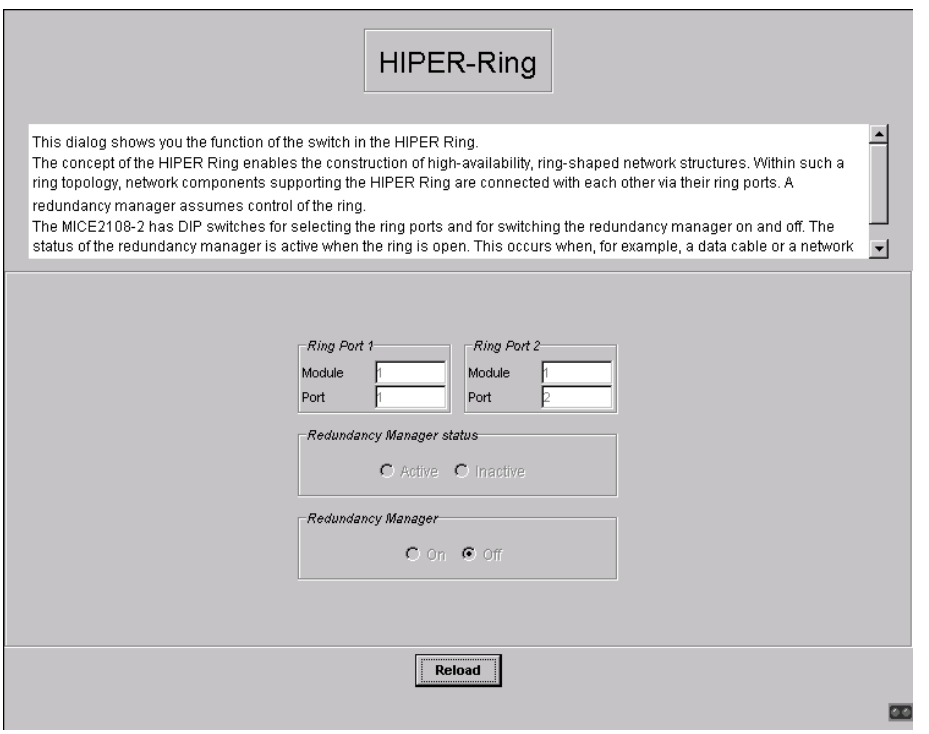


Fig. 62: Dialog HIPER-Ring

5.6.2 Setting port mirroring

This dialog allows you to configure and activate the port mirroring function of the switch. Port mirroring is when the data traffic of a source port is copied to a specified port. The data traffic at the source port is not influenced by port mirroring. A management tool connected at the specified port, e.g., an RMON probe, can thus monitor the data traffic of the source port.

Note: In active port mirroring, the specified port is used solely for observation purposes.

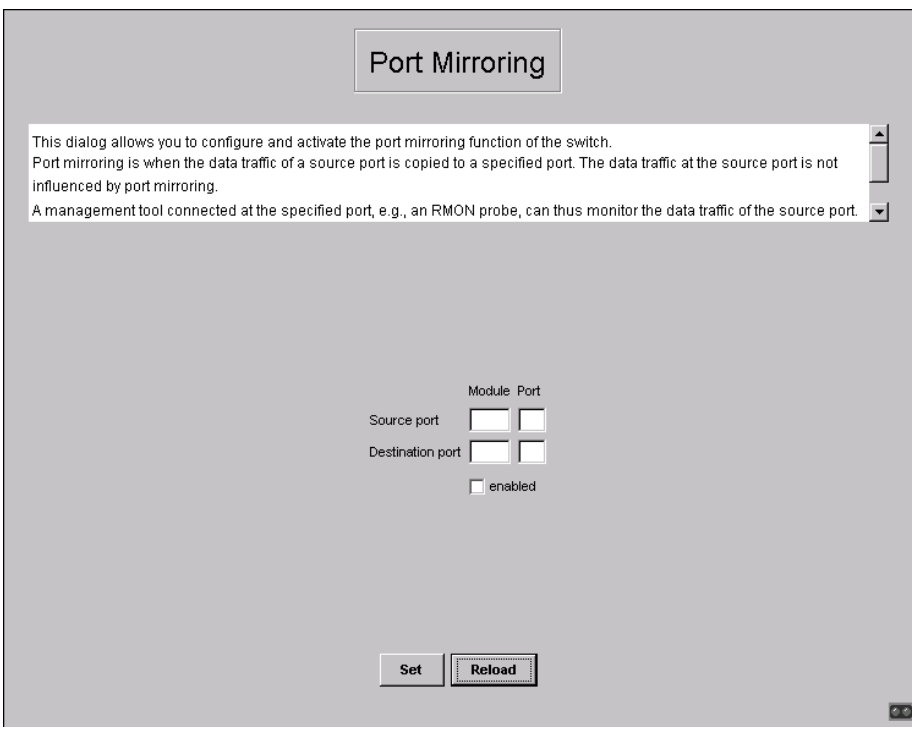


Fig. 63: Dialog Configure Port Mirroring

5.6.3 Switching the learning function on and off

This dialog allows you to monitor the data for all the ports. You mark the Disable Learning function to switch off the learning function of the MICE. Then the MICE will transfer all the data from each port to all the other ports.

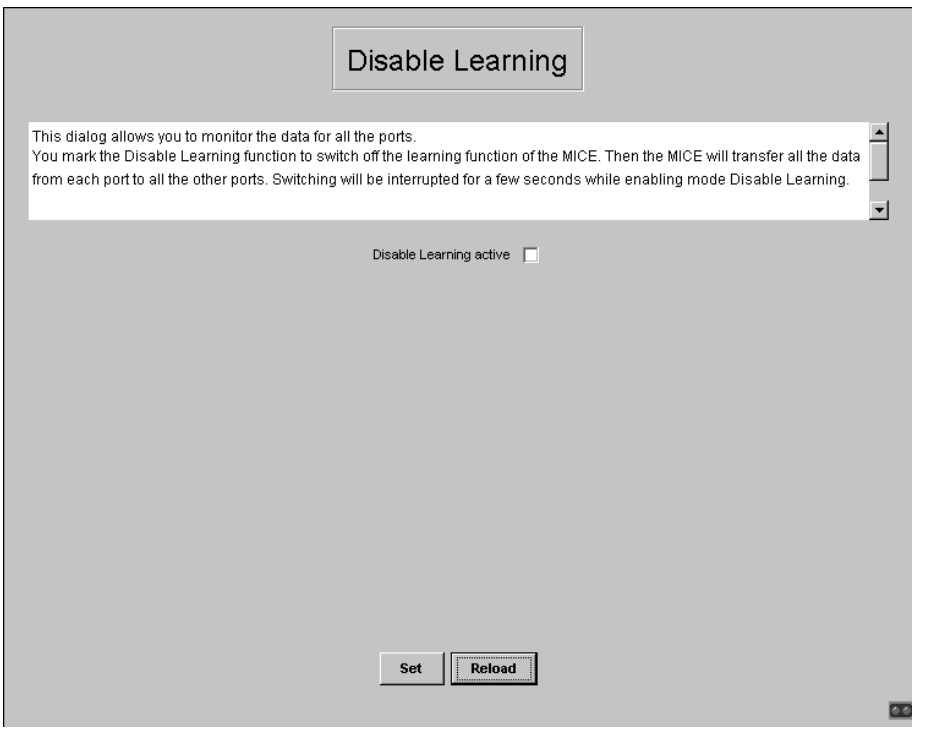


Fig. 64: Dialog Disable learning

5.6.4 Setting port security

In this dialog you can specify for each port from which terminal devices data can be received and sent to other ports. This function protects the network from unauthorized access.

- In the "Permitted MAC Address" column, you enter the MAC address of the device which can access the network via this port.
- The "Current MAC Address" column shows the MAC address of the device from which data was last received. By pressing the left mouse button, you can copy an entry from the "Current MAC Address" column into the "Permitted MAC Address" column.
- In the "Action" column you select whether an unauthorized access attempt should be followed by - no action (none) or - the sending of an alarm (trapOnly) or - the switching off of the port and the sending of an alarm (portDisable).

Note: An alarm (trap) can only be sent if at least one recipient is entered under Alarms (Traps) and both the appropriate status and "Authentication" are marked.

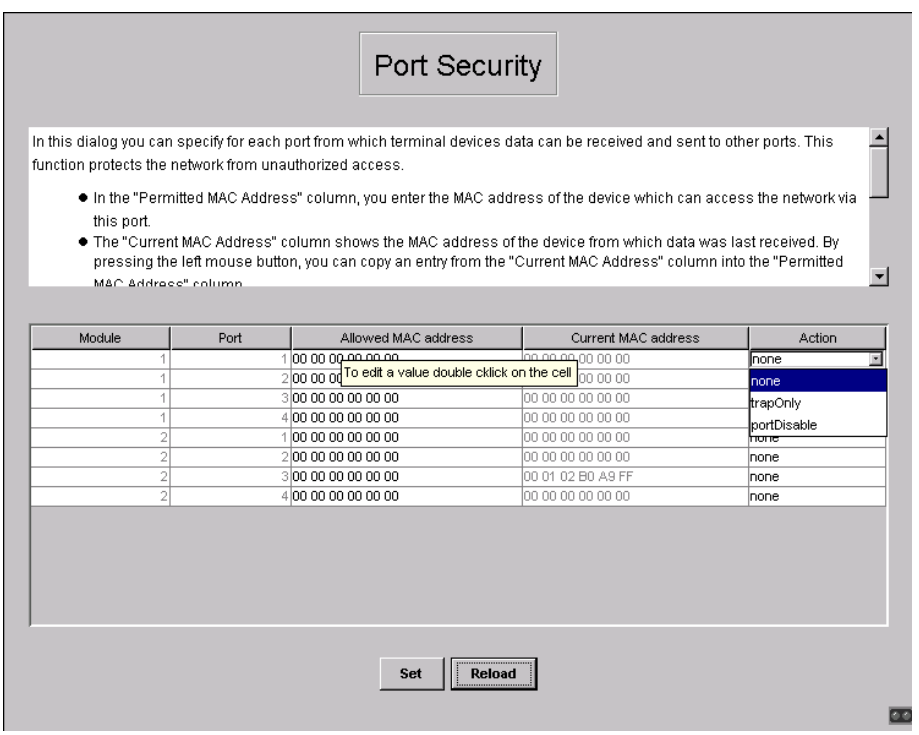


Fig. 65: Dialog Port Security

6 Management Information Base MIB

The **M**anagement **I**nformation **B**ase MIB is designed in the form of an abstract tree structure.
The branching points are the **object classes**. The “leaves” of the MIB are called **generic object classes**. Wherever necessary for unambiguous identification, the generic object classes are **instantiated**, i.e. the abstract structure is imaged on the reality, by specifying the port address or the source address.
Values (integers, timeticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The **object description** or **object ID** (OID) identifies the object class. The subidentifier (SID) is used for instantiation.

Example:
The generic object class

```
hmPSState (OID = 1.3.6.1.4.1.248.14.1.2.1.3)
```

is the description of the abstract information “power supply state”. It is, however, not possible to read any information from this, as the system does not know which power supply is meant.
Specification of the subidentifier (2) images this abstract information on the reality (instantiates it), which means that it refers to power supply 2. A value is assigned to this instance and can then be read. The instance “get `1.3.6.1.4.1.248.14.1.2.1.3`.2” for example, returns the response “1”, which means that the power supply is running correctly.

The following abbreviations are used in the MIB:

Comm	Group access rights
con	Configuration
Descr	Description
Fan	Fan
ID	Identifier
Lwr	Lower (e.g. threshold)
PS	Power supply
Pwr	Supply voltage

sys	System
UI	User Interface
Upr	Upper (e.g. threshold)
ven	Vendor (Hirschmann)

Definition of the syntax terms used:

Integer	An integer in the range 0 - 2^{32}
IP address	xxx.xxx.xxx.xxx (xxx = integer in the range 0-255)
MAC address	12-digit hexadecimal number in accordance with ISO / IEC 8802-3
Object Identifier	x.x.x.x… (e.g. 1.3.6.1.1.4.1.248…)
Octet String	ASCII character string
PSID	Power supply identifier (power supply number)
TimeTicks	Stopwatch Elapsed time (in seconds) = numerical value / 100 Numerical value = integer in the range 0 - 2^{32}
Timeout	Time value in hundredths of a second Time value = integer in the range 0-2^{32}
Type field	4-digit hexadecimal number in accordance with ISO / IEC 8802-3
Counter	Integer (0 - 2^{32}) whose value is incremented by 1 when certain events occur.

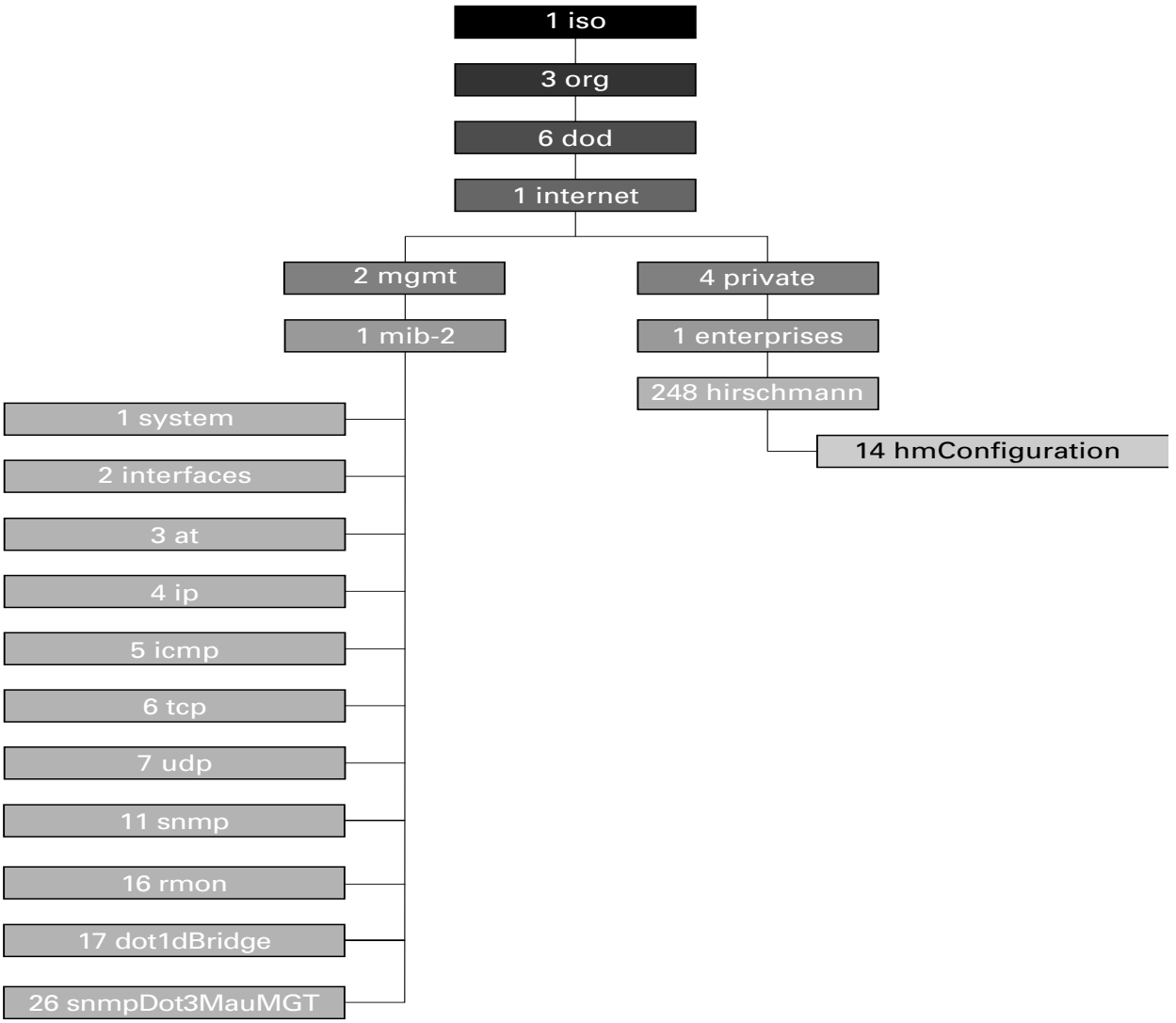


Fig. 66: Tree structure of the Hirschmann MIB

6.1 MIB II

6.1.1 System Group (1.3.6.1.2.1.1)

The system group is a required group for all systems. It contains system-related objects. If an agent has no value for a variable, then the response returned includes a string of length 0.

```
(1) system
    |-- (1) sysDescr
    |-- (2) sysObjectID
    |-- (3) sysUpTime
    |-- (4) sysContact
    |-- (5) sysName
    |-- (6) sysLocation
    |-- (7) sysServices
```

sysDescr

OID	1.3.6.1.2.1.1.1.0
Syntax	ASCII String (Size: 0-255)
Access	Read
Description	A verbal description of the entry. This value should contain the full name and version number of – type of system hardware, – operating system software, and – network software. The description must consist only of printable ASCII characters.

sysObjectID

OID1.3.6.1.2.1.1.2.0

Syntax	Object identifier
Access	Read
Description	The authorization identification of the manufacturer of the network management system that is integrated in this device. This value is placed in the SMI enterprises subtree (1.3.6.1.4.1) and describes which type of device is being managed. For example: if the manufacturer "Hirschmann GmbH" is assigned the subtree 1.3.6.1.4.1.248, then he can assign his bridge the identifier 1.3.6.1.4.1.2.248.2.1.

sysUpTime

OID	1.3.6.1.2.1.1.3.0
Syntax	Time ticks
Access	Read
Description	The time in 1/100 seconds since the last reset of the network management unit.

sysContact

OID1.3.6.1.2.1.1.4.0

Syntax	ASCII string (size: 0-255)
Access	Read and write
Description	The clear-text identification of the contact person for this managed node along with the information about how that person is to be contacted.

sysName

OID1.3.6.1.2.1.1.5.0

Syntax	ASCII string (size: 0-255)
Access	Read and write
Description	A name for this node for identifying it for administration. By convention, this is the fully qualified name in the domain.

sysLocation

OID	1.3.6.1.2.1.1.6.0
Syntax	ASCII string (size: 0-255)
Access	Read and write
Description	The physical location of this node (e.g. “staircase, 3rd floor”)

sysServices

OID	1.3.6.1.2.1.1.7.0
Syntax	Integer (0-127)
Access	Read
Description	This value designates the set of services offered by this device. It is the sum of several terms. For each layer of the OSI reference model there is one term of the form (2^{L-1}), where L identifies the layer. For example:

For a node that primarily performs routing functions the value would be $(2^{3-1}) = 4$.
For a node that is a host and which offers application services the value would be $(2^{4-1}) + (2^{7-1}) = 72$.

6.1.2 Interface Group (1.3.6.1.2.1.2)

The interface group contains information about the device interfaces.

(2) `interfaces`

```
|-- (1) ifNumber
|-- (2) ifTable
    |-- (1) ifEntry
        |-- (1) ifIndex
        |-- (2) ifDescr
        |-- (3) ifType
        |-- (4) ifMtu
        |-- (5) ifSpeed
        |-- (6) ifPhysAddress
        |-- (7) ifAdminStatus
        |-- (8) ifOperStatus
        |-- (9) ifLastChange
        |-- (10) ifInOctets
        |-- (11) ifInUcastPkts
        |-- (12) ifInNUcastPkts
        |-- (13) ifInDiscards
        |-- (14) ifInErrors
        |-- (15) ifInUnknownProtos
        |-- (16) ifOutOctets
        |-- (17) ifOutUcastPkts
        |-- (18) ifOutNUcastPkts
        |-- (19) ifOutDiscards
        |-- (20) ifOutErrors
        |-- (21) ifOutQLen
        |-- (22) ifSpecific
```

6.1.3 Address Translation Group (1.3.6.1.2.1.3)

The Address Translation Group is required for all systems. It contains information about the assignment of addresses.

(3) at

|-- (1) atTable
| |-- (1) atEntry
| | |-- (1) atIfIndex
| | |-- (2) atPhysAddress
| | |-- (3) atNetAddress

6.1.4 Internet Protocol Group (1.3.6.1.2.1.4)

The Internet Protocol Group is required for all systems. It contains information affecting IP switching.

(4) ip

|-- (1) ipForwarding
|-- (2) ipDefaultTTL
|-- (3) ipInReceives
|-- (4) ipInHdrErrors
|-- (5) ipInAddrErrors
|-- (6) ipForwDatagrams
|-- (7) ipInUnknownProtos
|-- (8) ipInDiscards
|-- (9) ipInDelivers
|-- (10) ipOutRequests
|-- (11) ipOutDiscards
|-- (12) ipOutNoRoutes
|-- (13) ipReasmTimeout
|-- (14) ipReasmReqds
|-- (15) ipReasmOKs
|-- (16) ipReasmFails
|-- (17) ipFragOKs

```
|
|-- (18) ipFragFails
|-- (19) ipFragCreates
|-- (20) ipAddrTable
|    |-- (1) ipAddrEntry
|         |-- (1) ipAdEntAddr
|         |-- (2) ipAdEntIfIndex
|         |-- (3) ipAdEntNetMask
|         |-- (4) ipAdEntBcastAddr
|         |-- (5) ipAdEntReasmMaxSize
|-- (21) ipRouteTable
|    |-- (1) ipRouteEntry
|         |-- (1) ipRouteDest
|         |-- (2) ipRouteIfIndex
|         |-- (3) ipRouteMetric1
|         |-- (4) ipRouteMetric2
|         |-- (5) ipRouteMetric3
|         |-- (6) ipRouteMetric4
|         |-- (7) ipRouteNextHop
|         |-- (8) ipRouteType
|         |-- (9) ipRouteProto
|         |-- (10) ipRouteAge
|         |-- (11) ipRouteMask
|         |-- (12) ipRouteMetric5
|         |-- (13) ipRouteInfo
|-- (22) ipNetToMediaTable
|    |-- (1) ipNetToMediaEntry
|         |-- (1) ipNetToMediaIfIndex
|         |-- (2) ipNetToMediaPhysAddress
|         |-- (3) ipNetToMediaNetAddress
|         |-- (4) ipNetToMediaType
|-- (23) ipRoutingDiscards
```

6.1.5 ICMP Group (1.3.6.1.2.1.5)

The Internet Control Message Protocol group is obligatory for all systems. It contains all the information on error handling and control for data exchange in the Internet.

(5) icmp

-- (1) icmpInMsgs
-- (2) icmpInMsgs
-- (3) icmpInDestUnreachs
-- (4) icmpInTimeExcds
-- (5) icmpInParmProbs
-- (6) icmpInSrcQuenchs
-- (7) icmpInRedirects
-- (8) icmpInEchos
-- (9) icmpInEchoReps
-- (10) icmpInTimestamps
-- (11) icmpInTimestampReps
-- (12) icmpInAddrMasks
-- (13) icmpInAddrMaskReps
-- (14) icmpOutMsgs
-- (15) icmpOutErrors
-- (16) icmpOutDestUnreachs
-- (17) icmpOutTimeExcds
-- (18) icmpOutParmProbs
-- (19) icmpOutSrcQuenchs
-- (20) icmpOutRedirects
-- (21) icmpOutEchos
-- (22) icmpOutEchoReps
-- (23) icmpOutTimestamps
-- (24) icmpOutTimestampReps
-- (25) icmpOutAddrMasks
-- (26) icmpOutAddrMaskReps

6.1.6 Transfer Control Protocol Group (1.3.6.1.2.1.6)

The Transfer Control Protocol group is required for all systems that have implemented TCP. Instances of objects that describe information about a particular TCP connection exist only as long as the connection exists.

(6) tcp

|-- (1) tcpRtoAlgorithm
|-- (2) tcpRtoMin
|-- (3) tcpRtoMax
|-- (4) tcpMaxConn
|-- (5) tcpActiveOpens
|-- (6) tcpPassiveOpens
|-- (7) tcpAttemptFails
|-- (8) tcpEstabResets
|-- (9) tcpCurrEstab
|-- (10) tcpInSegs
|-- (11) tcpOutSegs
|-- (12) tcpRetransSegs
|-- (13) tcpConnTable
| |-- (1) tcpConnEntry
| |-- (1) tcpConnState
| |-- (2) tcpConnLocalAddress
| |-- (3) tcpConnLocalPort
| |-- (4) tcpConnRemAddress
| |-- (5) tcpConnRemPort
|-- (14) tcpInErrs
|-- (15) tcpOutRsts

6.1.7 User Datagram Protocol Group (1.3.6.1.2.1.7)

The User Datagram Protocol group is required for all systems that have implemented UDP.

(7) udp

|-- (1) udpInDatagrams
|-- (2) udpNoPorts
|-- (3) udpInErrors
|-- (4) udpOutDatagrams
|-- (5) udpTable
| |-- (1) udpEntry
| | |-- (1) udpLocalAddress
| | |-- (2) udpLocalPort

6.1.8 Simple Network Management Protocol Group (1.3.6.1.2.1.11)

The Simple Network Management Protocol group is required for all systems. In SNMP installations that have been optimized to support either just one agent or one management station some of the listed objects will contain the value “0”

(11) snmp

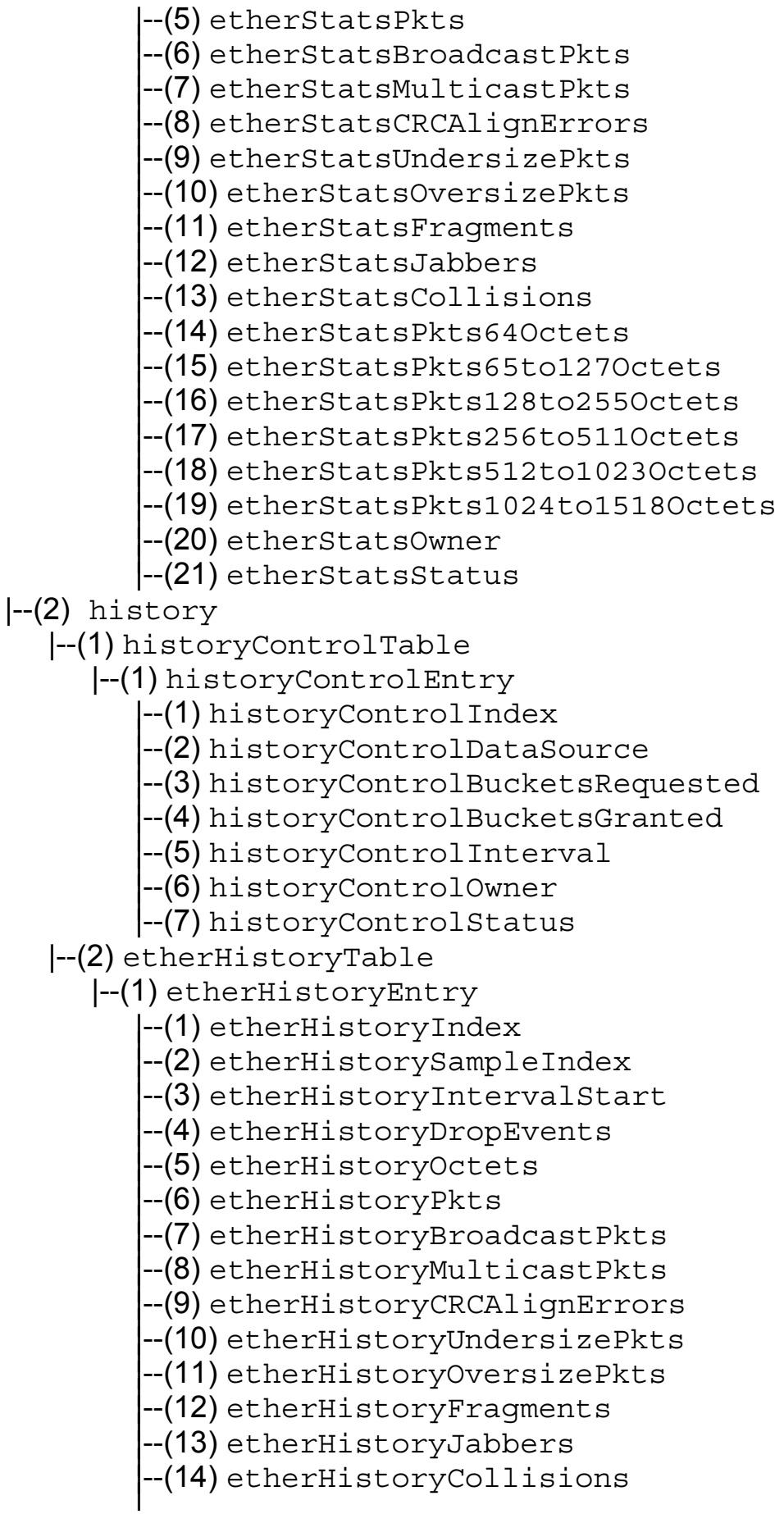
|-- (1) snmpInPkts
|-- (2) snmpOutPkts
|-- (3) snmpInBadVersions
|-- (4) snmpInBadCommunityNames
|-- (5) snmpInBadCommunityUses
|-- (6) snmpInASNParseErrs
|-- (7) not used
|-- (8) snmpInTooBigs
|-- (9) snmpInNoSuchNames
|-- (10) snmpInBadValues
|-- (11) snmpInReadOnlys

|-- (12) snmpInGenErrs
|-- (13) snmpInTotalReqVars
|-- (14) snmpInTotalSetVars
|-- (15) snmpInGetRequests
|-- (16) snmpInGetNexts
|-- (17) snmpInSetRequests
|-- (18) snmpInGetResponses
|-- (19) snmpInTraps
|-- (20) snmpOutTooBigs
|-- (21) snmpOutNoSuchNames
|-- (22) snmpOutBadValues
|-- (23) not used
|-- (24) snmpOutGenErrs
|-- (25) snmpOutGetRequests
|-- (26) snmpOutGetNexts
|-- (27) snmpOutSetRequests
|-- (28) snmpOutGetResponses
|-- (29) snmpOutTraps
|-- (30) snmpEnableAuthenTraps

6.1.9 RMON Gruppe (1.3.6.1.2.1.16)

This part of the MIB provides a continuous flow of current and historical network component data to the network management. The configuration of alarms and events controls the evaluation of network component counters. The agents inform the management station of the evaluation result by means of traps depending on the configuration.

(16) rmon
  |--(1) statistics
    |--(1) etherStatsTable
      |--(1) etherStatsEntry
        |--(1) etherStatsIndex
        |--(2) etherStatsDataSource
        |--(3) etherStatsDropEvents
        |--(4) etherStatsOctets


|--(5) etherStatsPkts
|--(6) etherStatsBroadcastPkts
|--(7) etherStatsMulticastPkts
|--(8) etherStatsCRCAlignErrors
|--(9) etherStatsUndersizePkts
|--(10) etherStatsOversizePkts
|--(11) etherStatsFragments
|--(12) etherStatsJabbers
|--(13) etherStatsCollisions
|--(14) etherStatsPkts64Octets
|--(15) etherStatsPkts65to127Octets
|--(16) etherStatsPkts128to255Octets
|--(17) etherStatsPkts256to511Octets
|--(18) etherStatsPkts512to1023Octets
|--(19) etherStatsPkts1024to1518Octets
|--(20) etherStatsOwner
|--(21) etherStatsStatus
|--(2) history
|--(1) historyControlTable
|--(1) historyControlEntry
|--(1) historyControlIndex
|--(2) historyControlDataSource
|--(3) historyControlBucketsRequested
|--(4) historyControlBucketsGranted
|--(5) historyControlInterval
|--(6) historyControlOwner
|--(7) historyControlStatus
|--(2) etherHistoryTable
|--(1) etherHistoryEntry
|--(1) etherHistoryIndex
|--(2) etherHistorySampleIndex
|--(3) etherHistoryIntervalStart
|--(4) etherHistoryDropEvents
|--(5) etherHistoryOctets
|--(6) etherHistoryPkts
|--(7) etherHistoryBroadcastPkts
|--(8) etherHistoryMulticastPkts
|--(9) etherHistoryCRCAlignErrors
|--(10) etherHistoryUndersizePkts
|--(11) etherHistoryOversizePkts
|--(12) etherHistoryFragments
|--(13) etherHistoryJabbers
|--(14) etherHistoryCollisions

```
        |--(15) etherHistoryUtilization
|--(3) alarm
   |--(1) alarmTable
      |--(1) alarmEntry
         |--(1) alarmIndex
         |--(2) alarmInterval
         |--(3) alarmVariable
         |--(4) alarmSampleType
         |--(5) alarmValue
         |--(6) alarmStartupAlarm
         |--(7) alarmRisingThreshold
         |--(8) alarmFallingThreshold
         |--(9) alarmRisingEventIndex
         |--(10) alarmFallingEventIndex
         |--(11) alarmOwner
         |--(12) alarmStatus
|--(9) event
   |--(1) eventTable
      |--(1) eventEntry
         |--(1) eventIndex
         |--(2) eventDescription
         |--(3) eventType
         |--(4) eventCommunity
         |--(5) eventLastTimeSent
         |--(6) eventOwner
         |--(7) eventStatus
   |--(2) logTable
      |--(1) logEntry (1)
         |--(1) logEventIndex
         |--(2) logIndex
         |--(3) logTime
         |--(4) logDescription
|--(22) switchRMON
   |--(1) smonMIBObjects
      |--(3) portCopyConfig
         |--(1) portCopyTable
            |--(1) portCopyEntry
               |--(1) portCopySource
               |--(2) portCopyDest
               |--(3) portCopyDestDropEvents
               |--(4) portCopyDirection
               |--(5) portCopyStatus
```

6.1.10 dot1dBridge (1.3.6.1.2.1.17)

This part of the MIB contains bridge-specific objects.

```
(17) dot1dBridge
   |--(1) dot1dBase
      |--(1) dot1dBaseBridgeAddress
      |--(2) dot1dBaseNumPorts
      |--(3) dot1dBaseType
      |--(4) dot1dBasePortTable
         |--(1) dot1dBasePortEntry
            |--(1) dot1dBasePort
            |--(2) dot1dBasePortIfIndex
            |--(3) dot1dBasePortCircuit
            |--(4) dot1dBasePortDelayExceededDiscards
            |--(5) dot1dBasePortMtuExceededDiscards
   |--(2) dot1dStp
   |--(3) dot1dSr
   |--(4) dot1dTp
      |--(1) dot1dTpLearnedEntryDiscards
      |--(2) dot1dTpAgingTime
      |--(3) dot1dTpFdbTable
         |--(1) dot1dTpFdbEntry
            |--(1) dot1dTpFdbAddress
            |--(2) dot1dTpFdbPort
            |--(3) dot1dTpFdbStatus
      |--(4) dot1dTpPortTable
         |--(1) dot1dTpPortEntry
            |--(1) dot1dTpPort
            |--(2) dot1dTpPortMaxInfo
            |--(3) dot1dTpPortInFrames
            |--(4) dot1dTpPortOutFrames
            |--(5) dot1dTpPortInDiscards
   |--(5) dot1dStatic
      |--(1) dot1dStaticTable
         |--(1) dot1dStaticEntry
            |--(1) dot1dStaticAddress
            |--(2) dot1dStaticReceivePort
            |--(3) dot1dStaticAllowedToGoTo
            |--(4)  dot1dStaticStatus
   |--(6) pBridgeMIB
      |--(1) pBridgeMIBObjects
```

```
        |--(1) dot1dExtBase
            |--(1) dot1dDeviceCapabilities
            |--(2) dot1dTrafficClassesEnabled
            |--(3) dot1dGmrpStatus
            |--(4) dot1dPortCapabilitiesTable
                |--(1) dot1dPortCapabilitiesEntry
                    |--(1) dot1dPortCapabilities
        |--(3) dot1dGarp
            |--(1) dot1dPortGarpTable
                |--(1) dot1dPortGarpEntry
                    |--(1) dot1dPortGarpJoinTime
                    |--(2) dot1dPortGarpLeaveTime
                    |--(3) dot1dPortGarpLeaveAllTime
        |--(4) dot1dGmrp
            |--(1) dot1dPortGmrpTable
                |--(1) dot1dPortGmrpEntry
                    |--(1) dot1dPortGmrpStatus
                    |--(2) dot1dPortGmrpFailedRegistrations
                    |--(3) dot1dPortGmrpLastPduOrigin
|--(7) qBridgeMIB
    |--(1) qBridgeMIBObjects
        |--(2) dot1qTp
            |--(3) dot1qTpGroupTable
                |--(1) dot1qTpGroupEntry
                    |--(1) dot1qTpGroupAddress
                    |--(2) dot1qTpGroupEgressPorts
                    |--(3) dot1qTpGroupLearnt
            |--(4) dot1qForwardAllTable
                |--(1) dot1qForwardAllEntry
                    |--(1) dot1qForwardAllPorts
                    |--(2) dot1qForwardAllStaticPorts
                    |--(3) dot1qForwardAllForbiddenPorts
            |--(5) dot1qForwardUnregisteredTable
                |--(1) dot1qForwardUnregisteredEntry
                    |--(1) dot1qForwardUnregisteredPorts
                    |--(2) dot1qForwardUnregisteredStaticPorts
                    |--(3) dot1qForwardUnregisteredForbiddenPorts
```

6.1.11 MAU Management Group (1.3.6.1.2.1.26)

The MAU Management Group is responsible for setting the autonegotiation parameters.

(26) snmpDot3MauMgt

- |--(2) dot3IfMauBasicGroup
  - |--(1) ifMauTable
    - |--(1) ifMauEntry
      - |-- (1) ifMauIfIndex
      - |-- (2) ifMauIndex
      - |-- (3) ifMauType
      - |-- (4) ifMauStatus
      - |-- (5) ifMauMediaAvailable
      - |-- (6) ifMauMediaAvailableStateExits
      - |-- (7) ifMauJabberState
      - |-- (8) ifMauJabberingStateEnters
      - |-- (9) ifMauFalseCarriers
      - |-- (10)ifMauTypeList
      - |-- (11)ifMauDefaultType
      - |-- (12)ifMauAutoNegSupported
- |--(5) dot3IfMauAutoNegGroup
  - |--(1) ifMauAutoNegTable
    - |-- (1) ifMauAutoNegEntry
      - |-- (1) ifMauAutoNegAdminStatus
      - |-- (2) ifMauAutoNegRemoteSignaling
      - |-- (4) ifMauAutoNegConfig
      - |-- (5) ifMauAutoNegCapability
      - |-- (6) ifMauAutoNegCapAdvertised
      - |-- (7) ifMauAutoNegCapReceived
      - |-- (8) ifMauAutoNegRestart

6.2 Private MIB

The private MIB is for configuring the device-specific properties of the MICE. The groups below are implemented in the MICE from the private MIB hmConfiguration (OID = 1.3.6.1.4.1.248.14).

- hmChassis (OID = 1.3.6.1.4.1.248.14.1)
- hmAgent (OID = 1.3.6.1.4.1.248.14.2)
- hmUserGroup (OID = 1.3.6.1.4.1.248.14.3)
- hmRingRedundancy (OID = 1.3.6.1.4.1.248.14.5)

6.2.1 Device group

The device group contains information on the status of the MICE hardware.

```
(14) hmConfiguration
   |--(1) hmChassis
      |--(1) hmSystemTable
         |--(1) hmSysProduct
         |--(2) hmSysVersion
         |--(3) hmSysGroupCapacity
         |--(4) hmSysGroupMap
         |--(5) hmSysMaxPowerSupply
         |--(6) hmSysMaxFan
         |--(7) hmSysGroupModuleCapacity
         |--(8) hmSysModulePortCapacity
         |--(9) hmSysGroupTable
            |--(1) hmSysGroupEntry
               |--(1) hmSysGroupID
               |--(2) hmSysGroupType
               |--(3) hmSysGroupDescription
               |--(4) hmSysGroupHwVersion
               |--(5) hmSysGroupSwVersion
               |--(6) hmSysGroupModuleMap
               |
```

```
            |--(7) hmSysGroupAction
            |--(8) hmSysGroupActionResult
        |--(10) hmSysModuleTable
            |--(1) hmSysModuleEntry
                |--(1) hmSysModGroupID
                |--(2) hmSysModID
                |--(3) hmSysModType
                |--(4) hmSysModDescription
                |--(5) hmSysModVersion
                |--(6) hmSysModNumOfPorts
                |--(7) hmSysModFirstMauIndex
        |--(11) hmInterfaceTable
            |--(1) hmIfEntry
                |--(1) hmIfaceGroupID
                |--(2) hmIfaceID
                |--(3) hmIfaceStpEnable
                |--(4) hmIfaceLinkType
                |--(5) hmIfaceAction
                |--(6) hmIfaceNextHopMacAddress
                |--(7) hmIfaceFlowControl
                |--(8) hmIfacePriorityThreshold
                |--(9) hmIfaceName
                |--(10) hmIfaceTrunkID
                |--(11) hmIfacePrioTOSEnable
                |--(12) hmIfaceBcastLimit
                |--(13) hmIfaceUtilization
                |--(14) hmIfaceUtilizationControlInterval
        |--(20) hmSysChassisName
        |--(21) hmSysStpEnable
        |--(22) hmSysFlowControl
        |--(23) hmSysBOOTPEnable
        |--(24) hmSysDHCPEnable
        |--(25) hmSysTelnetEnable
        |--(26) hmSysHTTPEnable
    |--(2) hmPSTable
        |--(1) hmPSEntry
            |--(1) hmPSSysID
            |--(2) hmPSID
            |--(3) hmPSState
    |--(5) hmCurrentAddressTable
        |--(1) hmCurrentAddressEntry
            |--(1) hmCurrentAddress
            |--(2) hmCurrentAddressReceivePort
            |
```

```
        |--(3) hmCurrentAddressStaticEgressPorts
        |--(4) hmCurrentAddressEgressPorts
        |--(5) hmCurrentAddressStatus
|--(10) hmRS2ext
    |--(1) hmRS2OperMode
    |--(2) hmRS2ConfigError
    |--(3) hmRS2SigRelayState
    |--(4) hmSigLinkTable
        |--(1) hmSigLinkEntry
            |--(1) hmSigLinkID
            |--(2) hmSigLinkAlarm
    |--(5) hmSigTrapReason
    |--(6) hmSigReasonIndex
    |--(7) hmRS2TopologyGroup
        |--(1) hmRS2PartnerIpAddress
        |--(2) hmRS2TopologyTable
            |--(1) hmRS2TopologyEntry
                |--(1) hmRS2TopologyLinkID
                |--(2) hmRS2TopologyIpAddress
    |--(9) hmRS2DisableLearningGroup
        |--(1) hmRS2DisableLearningStatus
```

6.2.2 Management group

The management group contains parameters for configuring the management agent.

```
(14)hmConfiguration
    |--(2) hmAgent
        |--(1) hmAction
        |--(2) hmActionResult
        |--(3) hmNetwork
            |--(1) hmNetLocalIPAddr
            |--(2) hmNetLocalPhysAddr
            |--(3) hmNetGatewayIPAddr
            |--(4) hmNetMask
            |--(7) hmNetAction
        |--(4) hmFSTable
            |--(1) hmFSUpdFileName
            |--(2) hmFSConfFileName
            |--(3) hmFSLogFileName
            |--(4) hmFSUserName
            |--(5) hmFSTPPassword
            |--(6) hmFSAction
            |--(8) hmFSActionResult
            |--(9) hmFSBootConfiguration
            |--(10) hmFSRunningConfiguration
            |--(11) hmFSLastMessage
            |--(200) hmAutoconfigGroup
                |--(1) hmAutoconfigAdapterStatus
        |--(7) hmAuthGroup
            |--(1) hmAuthHostTableEntriesMax
            |--(2) hmAuthCommTableEntriesMax
            |--(3) hmAuthCommTable
                |--(1) hmAuthCommEntry
                    |--(1) hmAuthCommIndex
                    |--(2) hmAuthCommName
                    |--(3) hmAuthCommPerm
                    |--(4) hmAuthCommState
            |--(4) hmAuthHostTable
                |--(1) hmAuthHostEntry
                    |--(1) hmAuthHostIndex
                    |--(2) hmAuthHostName
                    |--(3) hmAuthHostCommIndex
                    |
```

```
            |--(4) hmAuthHostIpAddress
            |--(5) hmAuthHostIpMask
            |--(6) hmAuthHostState
|--(8) hmTrapGroup
    |--(1) hmTrapCommTableEntriesMax
    |--(2) hmTrapDestTableEntriesMax
    |--(3) hmTrapCommTable
        |--(1) hmTrapCommEntry
            |--(1) hmTrapCommIndex
            |--(2) hmTrapCommCommIndex
            |--(3) hmTrapCommColdStart
            |--(4) hmTrapCommLinkDown
            |--(5) hmTrapCommLinkUp
            |--(6) hmTrapCommAuthentication
            |--(7) hmTrapCommBridge
            |--(8) hmTrapCommRMON
            |--(9) hmTrapCommUsergroup
            |--(10)hmTrapCommDualHoming
            |--(11)hmTrapCommChassis
            |--(12)hmTrapCommState
    |--(4) hmTrapDestTable
        |--(1) hmTrapDestEntry
            |--(1) hmTrapDestIndex
            |--(2) hmTrapDestName
            |--(3) hmTrapDestCommIndex
            |--(4) hmTrapDestIpAddress
            |--(5) hmTrapDestIpMask
            |--(6) hmTrapDestState
|--(9) hmLastAccessGroup
    |--(1) hmLastIpAddr
    |--(2) hmLastPort
    |--(3) hmLastCommunity
```

6.2.3 User groups group

The user groups group contains parameters for configuring the user group functions.

```
(14) hmConfiguration
    |--(3) hmUserGroup
        |--(4) hmPortSecurityTable
            |--(1) hmPortSecurityEntry
                |--(1) hmPortSecSlotID
                |--(2) hmPortSecPortID
                |--(3) hmPortSecPermission
                |--(4) hmPortSecAllowedUserID
                |--(5) hmPortSecAllowedGroupIDs
                |--(6) hmPortSecConnectedUserID
                |--(7) hmPortSecAction
```

6.2.4 HIPER-Ring redundancy group

The HIPER-Ring redundancy group contains parameters for configuring the HIPER-Ring redundancy.

```
(14) hmConfiguration
    |--(5) hmRingRedundancy
        |--(1) hmRingRedTable
            |--(1) hmRingRedEntry
                |--(1) hmRingRedPrimGroupID
                |--(2) hmRingRedPrimIfIndex
                |--(3) hmRingRedPrimIfOpState
                |--(4) hmRingRedRedGroupID
                |--(5) hmRingRedRedIfIndex
                |--(6) hmRingRedRedIfOpState
                |--(7) hmRingRedOperState
                |--(8) hmRingRedMode
```

7 User Interface

The User Interface offers users the option of choosing certain functions of the MICE management agent in a menu-driven way.

The following menu items can be selected:

- System parameters
- Switch Security
- Port Configuration / Statistics
- Disable Learning
- Configuration
- Update
- Password
- Ping
- System Reset

7.1 Starting the User Interface

☐ After connecting to the MICE with a VT100 terminal via V.24, press a key. A window will appear on the screen for entering the password. Only one user can access the User Interface.

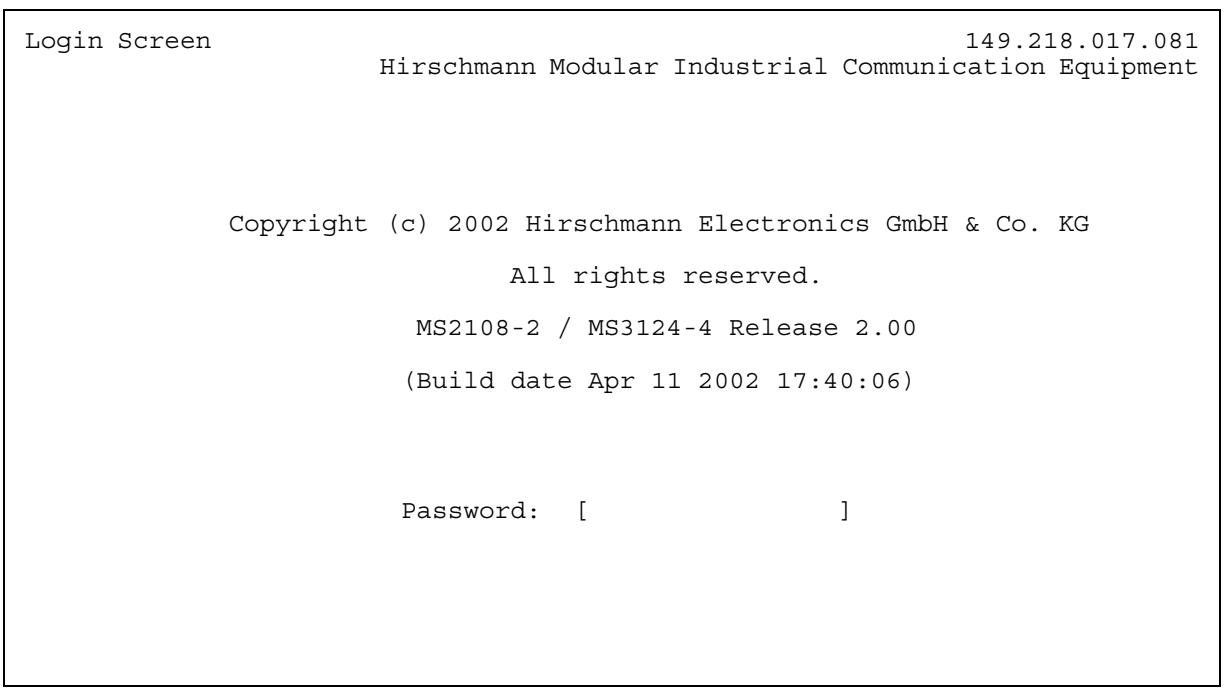


Fig. 67: Logging in to the User Interface program

☐ Enter the password. The default value for the password is **`private`**. You can change the password later in the User Interface (see “Password” on Page 201) or via the web interface. Please note that passwords are case-sensitive.

The main menu screen appears.

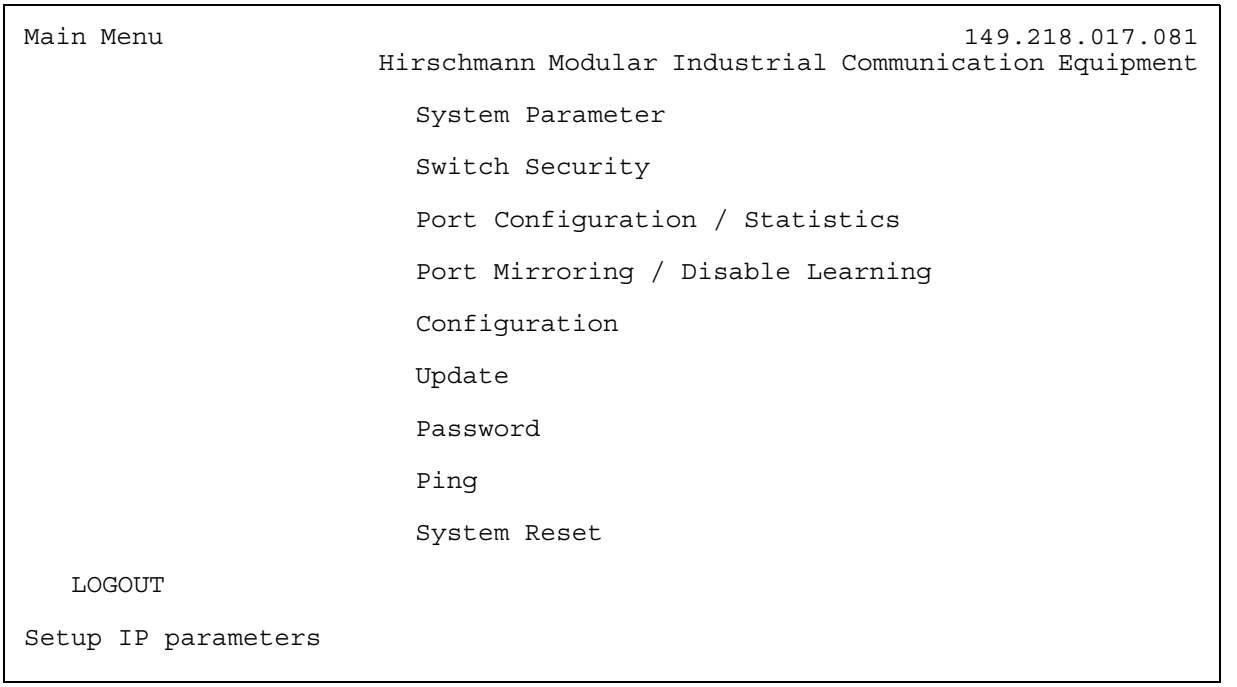


Fig. 68: Main menu

7.2 Working with the User Interface

- Use the arrow keys or the tab key to move the cursor.
- To change the specified values in a selection field, press the space bar.
- The new settings are accepted if the cursor is in the APPLY field, and the enter key is pressed.
- The bottom line contains a help text for the selected item.
- To exit the User Interface, select `LOGOUT` in the main menu and press the enter key.

The main menu consists of 9 submenus.

7.2.1 System parameters

This menu is for entering the

- IP address
- Subnet mask
- Gateway IP address

for displaying the MAC address of the MICE and

for enabling/disabling of BOOTP/DHCP.

```
System Parameter                                          149.218.017.081
                          Hirschmann Modular Industrial Communication
Equipment


                        IP Address       : [149.218.17.81  ]
                        Subnet Mask      : [255.255.240.0  ]
                        Default Gateway  : [149.218.20.94  ]

                        IP Configuration : < LOCAL >

                        MAC Address      : 00:80:63:00:06:15
                        System Name      : [Hirschmann MICE ]


                        Note:

                    Set IP-Configuration <LOCAL> to use manual settings.
                  APPLY changes the state of the objects immediately and
                       saves the state to Non Volatile Memory.


   MAIN MENU  APPLY

Enter agent IP address in decimal dot format (e.g., 149.218.19.69)
```

Fig. 69: Menu system parameters

- **IP address**
  Enter the IP address of this MICE here. The default setting of the address is 0.0.0.0.

- **Subnet mask**
  If you are working in a large network and are using subnet masks, you can specify the mask of the subnet, to which your MICE is connected, here. The default setting of the subnet mask is 0.0.0.0.

- **Gateway IP address**
  Enter the IP address of the gateway here with which the MICE is to address other subnets. If there is no such gateway, you can omit this entry. The default setting of the IP address is 0.0.0.0.

MAC address

This field displays the MAC address of the MICE.

IP Configuration

☐ Select the desired IP configuration mode. By pressing the space bar, the following options become available:

– `Local`
– `BOOTP`
– `DHCP`

After selecting APPLY, the mode is activated (see “Basic settings” on Page 63).

System name

☐ Assign your MICE the name of your choice (see “DHCP (dynamic host configuration protocol)” on Page 64).

7.2.2 Switch Security

This menu is for the configuring access to the web-based management.

– `Disable` does not allow any access via the web-based management
– `Enable` allows access via the web-based management.

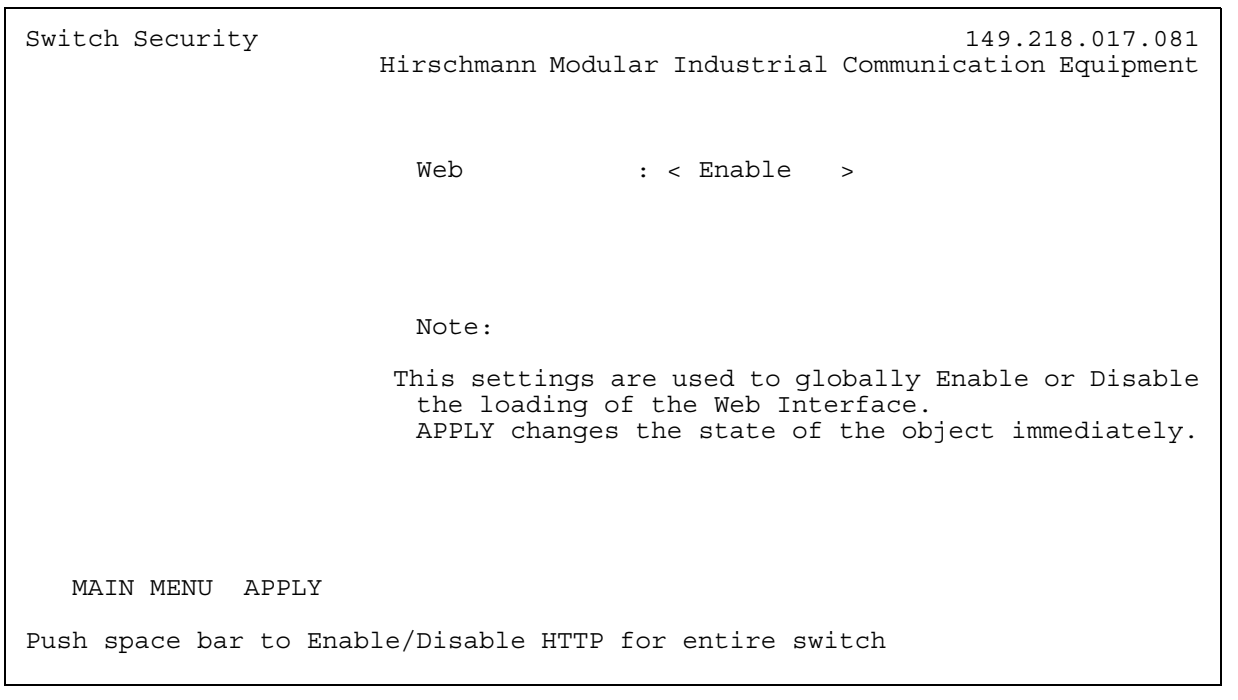


Fig. 70: Access control

7.2.3 Port Configuration / Statistics

This menu is for the configurating the port and displaying the port statistics

☐ First enter the module and port number and press the return key.

☐ You can enter the name of your choice for this port after `Port Name`.

- State
  - `Disable` disables the port
  - `Enable` enables the port
- Set Speed
  - `autonegotiate` enables the autonegotiation function
  - `10MHDX` 10 Mbit/s, half duplex
  - `10MFDX` 10 Mbit/s, full duplex
  - `100MHDX` 100 Mbit/s, half duplex
  - `100MFDX` 100 Mbit/s, full duplex

```
Port Configuration / Statistics                              149.218.017.081
                        Hirschmann Modular Industrial Communication Equipment

  Module.Port: 2.1    Port Name:  [                    ]

  State: <Enable   >  Set Speed:    <100MFDX       >
  Link:   Down        Actual Speed:  100MFDX         Type: 10/100 TP

  Port Statistics:

  Transmitted Packets:     0
  Received    Packets:     0
  Received    Bytes:       0
  Received    Broadcasts:  0
  Received    Multicasts:  0
  Received    Fragments:   0
  Detected    CRCErrors:   0
  Detected    Collisions:  0



  MAIN MENU   APPLY   REFRESH

Type in module number and press enter
```

Fig. 71: Menu Port Configuration

7.2.4 Port Mirroring / Disable Learning

This dialog gives you the option of viewing the data of all ports or of individual ports (monitoring).

- By selecting `Disable Learning`, you can disable the MICE learning function. Consequently, the MICE transmits all data from all ports to all ports.
- By selecting `Port Mirroring`, the MICE mirrors all send/receive data of the "Source Module.Ports" to the "Destination Module.Port". The MICE functions as a normal switch for the other ports.
- By selecting `Normal Switching`, you activate the MICE learning function, and it functions as a normal switch.

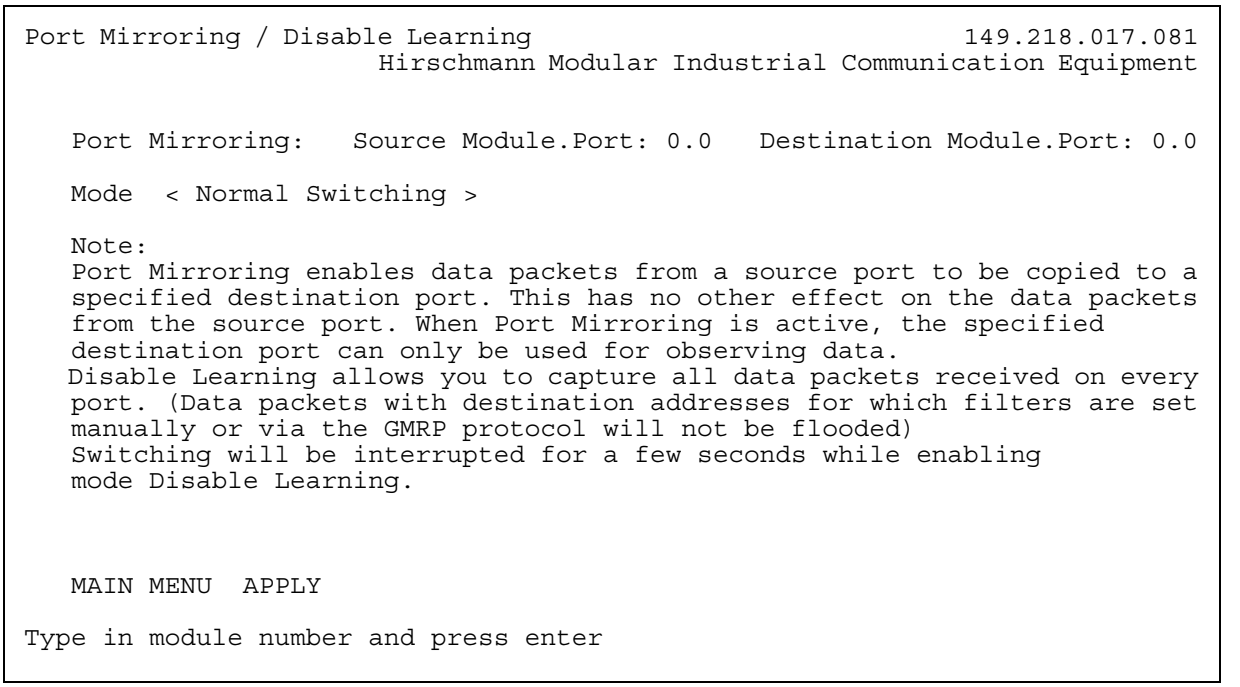


Fig. 72: Menu Disable Learning

7.2.5 Configuration

The MICE has two configuration settings:
- the default setting and
- the user-defined setting.

This submenu offers the option of storing a user-defined configuration. This configuration can be reloaded
– automatically when restarting or
– after restarting with the default settings

With `Load after reset` you can determine which configuration setting will be active after a restart:
– `default` loads the default configuration
– `local` loads the user-defined configuration from the flash memory,
– `remote` loads the user-defined configuration from the configuration file on the tftp server.

With `Load` you determine which configuration is to be loaded:
– `local` loads the user-defined configuration from flash memory,
– `remote` loads the user-defined configuration from the configuration file on the tftp server.

With `Save` you determine where the configuration setting is saved:
– `local` saves the user-defined configuration to flash memory,
– `remote` saves the user-defined configuration as a configuration file on the tftp server.
– `configadapter` saves the user-defined configuration in the AutoConfiguration Adapter and in the flash memory.

Any changes in this window are accepted by choosing `APPLY`.

The path for storing the configuration data is displayed in the line “URL.”. tftp is not able to create a new file. Therefore create an empty file on the tftp server before you “Save to URL“.

Example to save to a tftp server
☐ With any editor open a new file.
☐ Save the empty file to the appropriate path of the tftp server including the file name, e.g. `MICE/MICE_01.cfg`
☐ In line “URL“ enter the path of the tftp servr, e.g. `tftp://149.218.076.214/MICE/MICE_01.cfg`.

Note: The configuration file includes all configuration data including the password. Therefore pay attention to the access rights on the tftp server.

```
Save/Load Configuration                                    149.218.017.081
                      Hirschmann Modular Industrial Communication Equipment


   Load after reset:  <default configfile>

   Load:              <  local configfile>

   Save:              <  local configfile>


   URL of remote configuration file:  (e.g.: tftp://149.218.16.2/config.dat)
   [tftp://149.218.31.106/icc/ms2108-2_2_4tx_default.dat                    ]


   To load MIB-configuration after reset    APPLY Load after reset
   To load MIB-configuration                APPLY Load
   To save your current MIB-configuration   APPLY Save



   MAIN MENU   APPLY Load after reset   APPLY Load   APPLY Save

Push space bar to select default, local or remote configuration file
```

Fig. 73: Menu Save/Load Configuration

The selection of the AutoConfiguration Adapter (ACA) for a memory operation opens a new window - after you choose `Apply Save` - with the request:

☐ Pull the terminal block off the MICE and connect the ACA to the V.24 connection of the MICE.

Then the MICE performs the memory operation. The unlabeled LEDs indicate the status of the memory operation.

The transition of the LED's from a flashing to a static state indicates the end of the memory operation.

☐ To go back to using the user interface, pull the ACA from the MICE and connect the terminal block to the V.24 connection of the MICE.

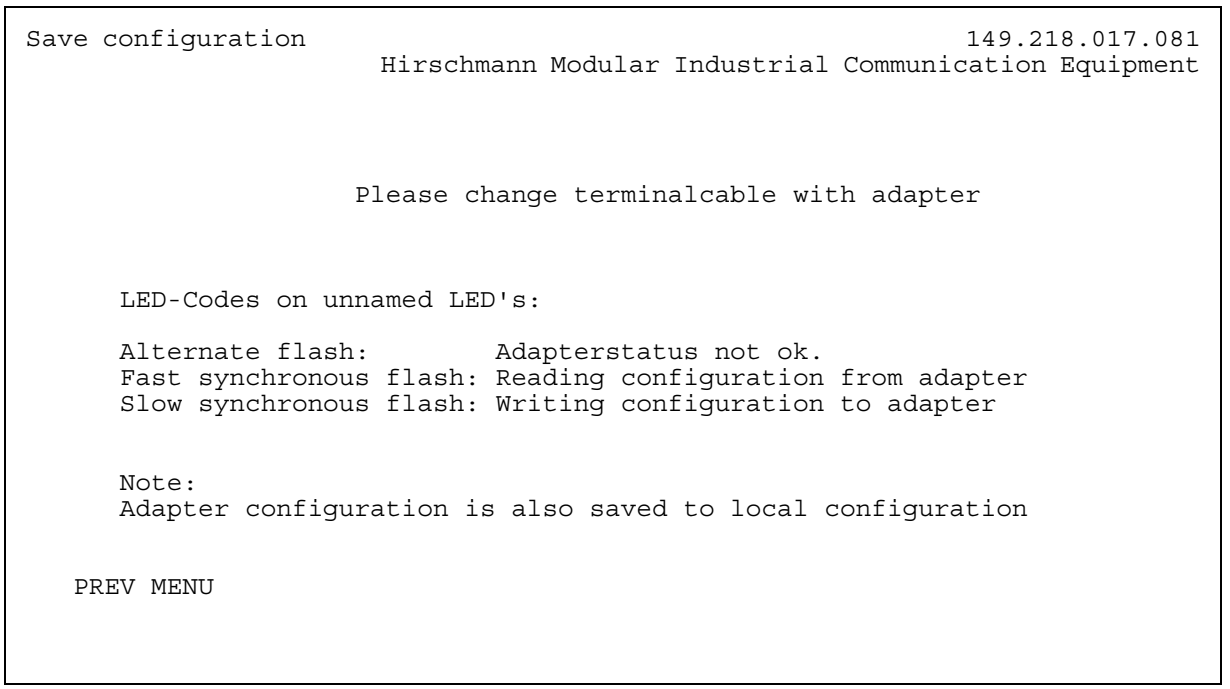


Fig. 74: Menu Memory operation AutoConfiguration Adapter

7.2.6 Updating

Before you can update the software, you need to know the correct location (pathname) of the update file.

☐ Enter the correct pathname in the field `URL of update file` and then press the enter key.

In the `Reset` line you can determine if you want the MICE to perform a restart after updating .

Choose `Apply` to start the update. It is active after a restart.

```
Update software                                          149.218.017.081
                          Hirschmann Modular Industrial Communication
Equipment


   URL of update file:
   [tftp://149.218.31.106/icc/k3.bin                                    ]

   A correct URL is for example:  (tftp://149.218.16.5/mice/mice.bin)


   Automatic Reset :  < Disable  >



   Note:

   APPLY saves the URL to Non Volatile Memory and starts the Update.



   MAIN MENU   APPLY

Enter URL of remote update file
```

Fig. 75: Menu Update MICE

7.2.7 Password

To protect your MICE from unauthorized access, change the password in this submenu.

- ☐ Enter your old password in the field `Old Password` and press the enter key.
- ☐ Enter your new password in the field `New Password` and press the enter key.
- ☐ Repeat the entry of your new password in the field `Retype password` and press the enter key.
- ☐ To accept the new password, choose `APPLY` and then press the enter key.
- ☐ To ensure that the new password is available after a restart, save the configuration (see “Configuration” on Page 197).

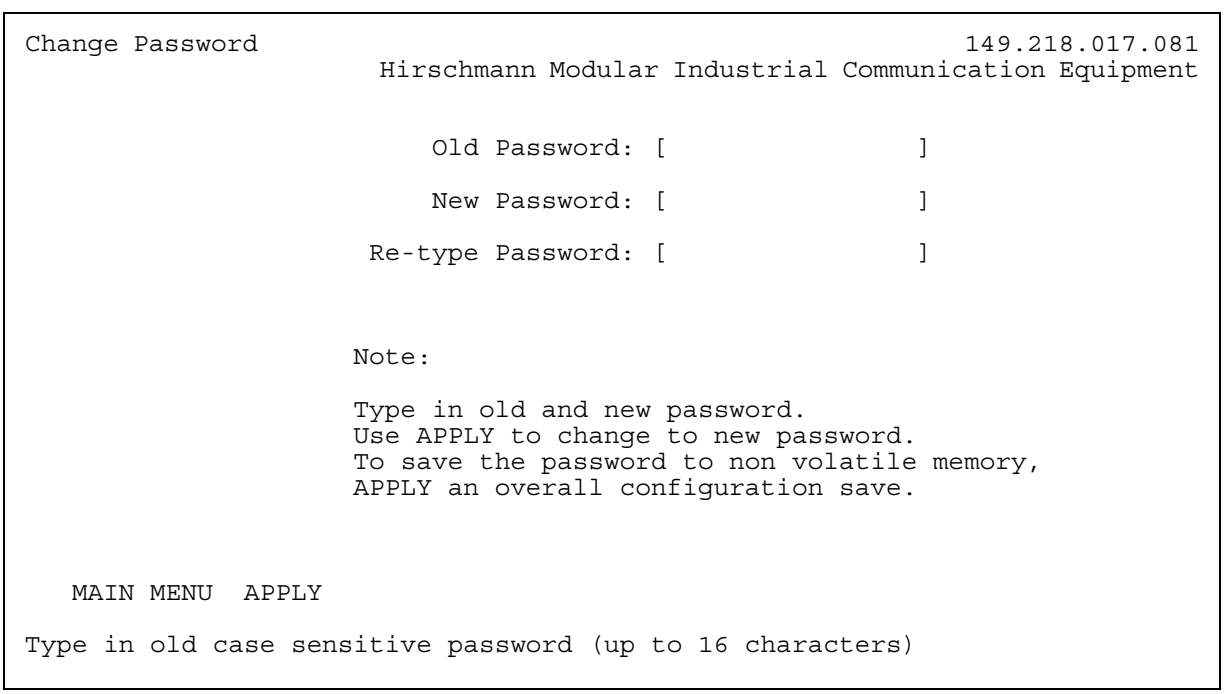


Fig. 76: Menu Change Password

7.2.8 Ping

In the Ping menu you can test the accessibility of another network station.

☐ In the `IP address of the host` field enter the IP address of the desired station, and then press the enter key.

Choose `Apply` to ping the desired station.

Depending on the accessibility of the station, you will receive the response:

`Host alive` or
`Host not alive`.

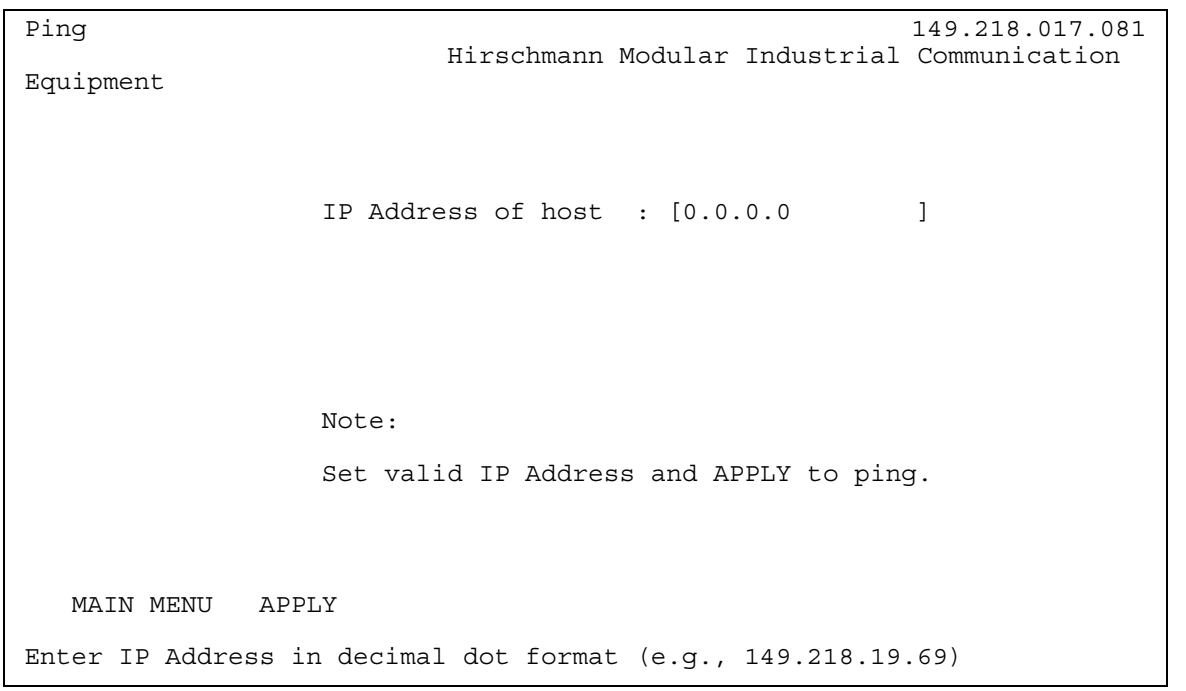


Fig. 77: Menu Ping

7.2.9 System Reset

☐ To reset select the `Confirm Reset` line.
By pressing the space bar the setting changes from `No` to `Yes`. Chose `APPLY` to reset the MICE.

```
System Reset                                                149.218.017.081
                        Hirschmann Modular Industrial Communication Equipment


             WARNING:
                       This will cause all connectivity to
                       the switch to be lost until the switch
                       has rebooted.


             Confirm Reset:  < No  >









   PREV MENU  APPLY

Push space bar to select 'yes' and reset the switch
```

Fig. 78: Menu System Reset

A Appendix

FAQ

Answers to frequently asked questions can be found at the Hirschmann Web site:

www.hirschmann.de

The heading FAQ with HiVision is located on the SERVICES pages in the Division Automation and Network Solutions area.

Based specifications and standards

List of norms and standards:

- EN 61000-6-2:1999 Basic standard - interference resistance in industry
- EN 55022:1998 - Interference characteristics for IT systems
- EN 60950:1997 - Security in IT systems
- EN 61131-2:1994 - Programmable Logic Controllers
- CFR-47 Part 15:1997 – Code of Federal Regulations
- Germanischer Lloyd Guidelines for the Performance of Type Tests Part 1
- UL 508:1998 – Underwriters Laboratories Inc. Standard for Safety

List of RFC's

- RFC 768 (UDP)
- RFC 783 (TFTP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 951 (BOOTP)
- RFC 1157 (SNMPv1)
- RFC 1155 (SMIv1)
- RFC 1213 (MIB2)
- RFC 1493 (Dot1d)
- RFC 1542 (BOOTP extensions)
- RFC 1757 (RMON)
- RFC 1945 (HTTP/1.0)
- RFC 2131 (DHCP)
- RFC 2132 (DHCP options)
- RFC 2239 (MAU MIB)
- RFC 2674 (Dot1p/Q)

IEEE-Normen

IEEE 802.1 D	Switching, GARP, GMRP, Spanning Tree
IEEE 802. Q	Tagging
IEEE 802.3	Ethernet

Certifications

Application for certification has been submitted for:
UL 508 / CSA C22.2 No.142
Standard for Safety - Industrial Control Equipment

Application for certification has been submitted for:
UL 1604 / CSA C22.2 No.950
Electrical Equipment for Use in Hazardous Locations

Application for certification has been submitted for:
UL 60950 / CSA C22.2 No.950
Safety of Information Technology Equipment,

Application for certification has been submitted for:
Germanischer Lloyd Baumusterprüfungen
Regulation for the Use of Computers and Computer Systems

Technical Data

MS2108 - 2

Dimensions W x H x D	120 x 134 x 99 mm 4.7 in x 5.3 in x 3.9 in
Weight	1 kg, 2.2 lb

MS3124 - 4

Dimensions W x H x D	275 x 134 x 140 mm 10.8 in x 5.3 in x 5.5 in
Weight	1.9 kg, 4.2 lb

Power supply

Operating voltage	24 VDC, -25% +33% safety extra-low voltage (SELV/PELV) redundant inputs decoupled
Power consumption	
MS2108 - 2	8,0 W
MS3124 - 4	11,0 W
MM2 - 2FXM2	3,4 W
MM2 - 2FXS2	3,4 W
MM2 - 2FXM3/2TX1	3,4 W
MM2 - 4FXM3	7,0 W
MM2 - 4TX1	0,8 W
MM2 - 2FLM4	2,6 W
MM3 - 4FLM4	5,0 W
MM3 - 2FXM2/2TX1	3,4 W
MM3 - 2FXS2/2TX1	3,4 W
MM3 - 1FXL2/3TX1	3,4 W
MM3 - 4FXM2	7,0 W
MB3 - 2T	0 W
Overload current protection at input	non-changeable thermal fuse

Environment

Ambient temperature	0 °C to 55 °C (with MM2 - 4FXM3: 0 °C to 50 °C)
Storage temperature	-20 °C to +80 °C
Relative humidity	10% to 95% (non condensing)
Atmospheric pressure	up to 795 hPa

Protection classes

Laser protection	Class 1 in compliance with EN 60825
Protection class	IP 20
Radiated emission	CFR-47 Part 15 Class A, Germanischer Lloyd Guidelines for the Performance of Type Tests Part 1 EN 55022 Class A Warning! This is a Class A device. This equipment may cause radio interference if used in a residential area. In this case the operator may be required to take appropriate measures.
Interference proof	
Discharge of static electricity	
Contact discharge	EN 61000-4-2 Test level 3
Air discharge	EN 61000-4-2 Test level 3
Electromagnetic fields	EN 61000-4-3 Test level 3
Fast transients	EN 61000-4-4 Test level 3
Surge voltage symmetrical	EN 61000-4-5 Test level 2
Surge voltage asymmetrical	EN 61000-4-5 Test level 3
Cable-based RF faults	EN 61000-4-6 Test level 3
Stability	
Vibration	IEC 60068-2-6 Test FC, testing level in line with IEC 61131-2 E2 CDV and Germanischer Lloyd Guidelines for the Performance of Type Tests Part 1
Shock	IEC 60068-2-27 Test Ea, testing level in line with IEC 61131-2 E2 CDV

Network size

TX port 100BASE-TX	
Length of a TP segment	100 m (328 ft) typical

F/O ports 10BASE-FL according to IEEE 802.3 10BASE-FL

System attenuation	
50/125 µm fiber, multimode	11 dB (-FLM4)
62,5/125 µm fiber, multimode	14 dB (-FLM4)
Wave length	850 nm (-FLM4)

Example for F/O line length	
50/125 µm fiber, multimode	2.6 km (8,530 ft) maximum data of fiber: 3 dB/km, 400 MHz*km
62,5/125 fiber, multimode	3.6 km (11,811 ft) maximum data of fiber: 3.2 dB/km, 200 MHz*km

F/O ports 100BASE-FX according to IEEE 802.3u 100BASE-FX

System attenuation	
50/125 µm fiber, multimode	8 dB (-FXM2; -FXM3)
62,5/125 µm fiber, multimode	11 dB (-FXM2; -FXM3)
10/125 µm fiber, singlemode	16 dB (-FXS2)
Wave length	1300 nm (-FXM2; -FXM3; -FXS2)
10/125 µm fiber, singlemode	7-29 dB (-FXL2)
Wave length	1550 nm (-FXL2)

Example for F/O line length	
50/125 µm fiber, multimode	5 km (16,400 ft) maximum (-FXM2; -FXM3) data of fiber: 1 dB/km, 800 MHz*km
62,5/125 fiber, multimode	4 km (13,120 ft) maximum (-FXM2; -FXM3) data of fiber at 1300 nm: 1 dB/km, 500 MHz*km
10/125 µm fiber, singlemode	30 km (98,420 ft) maximum (-FXS2) data of fiber: 0,4 dB/km
10/125 µm-Faser, singlemode	24-100 km (78,740-328,083 ft) (-FXL2) data of fiber at 1550 nm, 0,3 dB/km

Scope of delivery

MS2108 - 2 incl.	terminal block for power supply MICE manual on CDROM Labels Description & operation instructions
MS3124 - 4 incl.	terminal block for power supply MICE manual on CDROM Labels Description & operation instructions

Order number

MS2108 - 2	943 717-001
MM2 - 2FLM4	943 734-001
MM2 - 4TX1	943 722-001
MM2 - 4FXM3	943 721-001
MM2 - 2FXM3 / 2TX1	943 720-001
MM2 - 2FXM2	943 718-001
MM2 - 2FXS2	943 719-001
MS3124 - 4	943 746-001
MM3 - 4FLM4	943 760-001
MM3 - 2FXM2/2TX1	943 761-001
MM3 - 2FXS2/2TX1	943 762-001
MM3 - 1FXL3/3TX1	943 763-001
MM3 - 4FXM2	943 764-001
MB3 - 2T	943 733-001

Accessories

Network Management Software HiVision	943 471-100
Manal "Basics INDUSTRIAL ETHERNET and TCP/IP"	280 720-834
Terminal access cable	943 301-001
AutoConfiguration Adapter ACA 11	943 751-001
Rail Power Supply RPS 60	943 662-001
Rail Power Supply RPS 120	943 662-011

Literature references

[1] “Optische Übertragungstechnik in der Praxis”
Christoph Wrobel
Hüthig Buch Verlag Heidelberg
ISBN 3-7785-2262-0

[2] Hirschmann Manual
“Management MIKE”
943 416-001

[3] Hirschmann Manual
“Basics Line INDUSTRIAL ETHERNET and TCP/IP”
280 720-834

[4] Hirschmann Manual
“MultiLAN Switch”
943 309-001

[5] Hirschmann Manual
“ETHERNET”
943 320-001

Reader's comments

What is your opinion of this manual? We constantly strive to provide as comprehensive a description as possible of our product and provide important information to ensure trouble-free operation. Your comments and suggestions help us improve the quality of our documentation.

Your **assessment** of this manual:

	excellent	good	satisfactory	adequate	poor
Accuracy	O	O	O	O	O
Readability	O	O	O	O	O
Comprehensibility	O	O	O	O	O
Examples	O	O	O	O	O
Structure/Layout	O	O	O	O	O
Completeness	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover an error in the manual?
If so, on what page?

.....

.....

.....

.....

.....

.....

.....

Suggestions for improvement and additional information:

.....

.....

.....

.....

General comments:

.....

.....

.....

.....

Company / Department .....

Name / Telephone number .....

Street .....

Zip code / City .....

Date / Signature .....

Dear User,

Please fill out and return this page

- by fax to the number +49 (0)7127/14-1798 or
- by mail to

  Hirschmann Electronics GmbH & Co. KG
  Department AMM
  Stuttgarter Str. 45 - 51
  72654 Neckartenzlingen
  Germany

Index

A

abbreviations 161
ACA 59, 70, 104, 117, 136, 144, 198
access 144, 194
access right 116
Address Translation 169
agent 117, 130, 187
alarm 118, 129, 144, 159
alarm messages 117
Ambient temperature 50
applet 119
Authentication 144, 159
AutoConfiguration Adapter 59, 117, 135, 144, 197, 198
autonegotiation 58, 97, 112, 148, 195

B

Basic module 131
BOOTP 63, 138, 191, 193
browser 119, 121

C

Cascading 111
Chassis 144
Cold Start 144
Community 116
Configuration 135
configuration 71, 197
configuration data 63
Configuration file 135
configurations modifications 117
Control line 60
Counter 162

D

Destination address 151
destination address 75
DHCP 63, 138, 191, 193
DHCP client 64
DoD 72

E

EN60950 49
event counters 149

F

FAQ 207
Filter table 152
flash memory 197
full duplex 97, 112, 195

G

GARP 113, 152
Gateway 71, 192
generic object class 161
Global GMRP 153
GMRP 113, 114, 151, 152
GMRP packet 153
GMRP per port 153
Ground 50, 56
Ground cable 60
Ground screw 60

H

half duplex 97, 195
hardware address 64
hardware reset 117
HIPER-Ring 144, 154
history 129
http 132

I

ICMP 171
IEC950 49
initialization 99
instantiated 161
interface group 168
Internet Control Message 171
Internet Protocol Group 169
IP address 64, 69, 71, 72, 77, 192
IP configuration 193
ISO/IEC 27
ISO/OSI 75

J

Java 121
Javascript 121

L

language 122
learned address 108
Learning 158, 196
link down 117, 144
Link up 144
link-test pulses 98
login 121

M

MAC address 75, 159, 191, 193
MAC destination 76
MDI-X 58, 98

media module 144
message 117
MIB 161
ModuleMapChange 144
Monitoring 196
Multicast 113
Multicast address 152

N
National Electrical Code 49
network address 72
Network Information Center 72
Network management 114
network mask 71

O
object class 161
object description 161
object ID 161
Object Identifier 162

P
Password 135
password 71, 122, 140, 189, 201
PELV 49
Ping 202
polarity 98
polling 117
port mirroring 157
Port Security 144
Power Supply 144
priority 109

R
Receiving port 151
redundancy manager 144
redundant 102, 112
Reset 151, 203
reset 99
Restart 135, 136
restart 145, 149, 200
ring 112
Ring port 154
ring structure 112
RM Function 112

S
Safety extra-low voltage 49
SELV 49
Shielding ground 49
signal contact 54, 102, 144
Signaling Relay 144
Simple Network Management Protocol 173
Snap-in guide 56
SNMP 116, 117, 119, 173
SNMP management 119
software 81, 83
source address 75, 107
Standby 144
State on delivery 135
state on delivery: 116
store-and-forward 27
subidentifier 161
subnet 192
subnetwork 107
supply voltage 54, 102, 144
system group 165
System name 130
system name 64
System parameters 130

T
tag 109
Target address 152
TCP 172
TCP/IP 119
Terminal block 55
Terminal cable 60
tftp 132
Timeout 162
TimeTicks 162
traffic classes 108
Transfer Control Protocol 172
transfer parameters 70
Transmission security 117
trap 144
Trap destination table 117
traps 117
type field 109, 162

U
UDP 173
update 132, 200
User Datagram Protocol 173

V
V.24 189
V.24 connection 59
V.24 interface 59
VDE0805 49
VLAN 109
VT100 59, 69, 189

W
watchdog 97, 99
web management 97
Web site 122
web-based 119

web-based management 194

HIRSCHMANN